AWS Key Management Service meilleures pratiques

AWS Directives prescriptives

AWS Directives prescriptives: AWS Key Management Service meilleures pratiques

Table of Contents

AWS Key Management Service meilleures pratiques

Amazon Web Services (contributeurs)

Mars 2025 (historique du document)

AWS Key Management Service (AWS KMS) est un service géré qui vous permet de créer et de contrôler facilement les clés cryptographiques utilisées pour protéger vos données. Ce guide décrit comment l'utiliser efficacement AWS KMS et fournit les meilleures pratiques. Il vous permet de comparer les options de configuration et de choisir l'ensemble le mieux adapté à vos besoins.

Ce guide contient des recommandations sur la manière dont votre organisation peut AWS KMS protéger les informations sensibles et implémenter la signature pour de multiples cas d'utilisation. Il prend en compte les recommandations actuelles qui utilisent les dimensions suivantes :

- Gestion des clés — Options de délégation pour la gestion et les choix de stockage des clés
- Protection des données — Chiffrer les données au sein de vos propres applications plutôt que de le Services AWS faire en votre nom
- Gestion des accès : utilisation de politiques AWS KMS clés et de politiques AWS Identity and Access Management (IAM) pour mettre en œuvre un contrôle d'accès basé sur les rôles (RBAC) ou un contrôle d'accès basé sur les attributs (ABAC).
- Architecture multicompte et multirégion : recommandations pour les déploiements à grande échelle.
- Facturation et gestion des coûts — Compréhension de vos coûts et de votre utilisation, et recommandations sur les moyens de réduire les coûts.
- Detective Controls : surveillance de l'état de vos clés KMS, de vos paramètres de chiffrement et de vos données chiffrées.
- Réponse aux incidents : correction des erreurs de configuration qui entraînent le non-respect de vos politiques de protection des données.

Résultats commerciaux ciblés

Vos données constituent un actif critique et sensible pour votre entreprise. Avec AWS KMS, vous gérez les clés cryptographiques utilisées pour protéger et vérifier vos données. Vous contrôlez la manière dont vos données sont utilisées, qui y a accès et comment elles sont cryptées. Ce guide est destiné à aider les développeurs, les administrateurs système et les professionnels de la sécurité

à mettre en œuvre les meilleures pratiques de chiffrement qui vous aident à sécuriser les données sensibles stockées ou transmises par le biais de ce dernier Services AWS. En comprenant et en mettant en œuvre les recommandations de ce guide, vous pouvez promouvoir la confidentialité et l'intégrité des données dans votre AWS environnement. Vous pouvez répondre à vos exigences en matière de protection des données, que ces exigences soient formulées en interne ou que vous ayez des exigences spécifiques à un programme de conformité ou de validation. Pour plus d'informations sur la manière dont vous AWS KMS pouvez sécuriser les données dans votre AWS environnement, consultez la section Utilisation du AWS KMS chiffrement Services AWS dans la AWS KMS documentation.

À propos AWS KMS keys

AWS Key Management Service (AWS KMS) vous permet de créer des clés cryptographiques qui peuvent être utilisées sur les données que vous transmettez au service. Le type de ressource principal est la clé KMS, dont il existe trois types :

- Clés symétriques AES (Advanced Encryption Standard) : il s'agit de clés de 256 bits utilisées dans le mode Galois Counter Mode (GCM) d'AES. Ces clés fournissent un chiffrement et un déchiffrement authentifiés des données dont la taille est inférieure à 4 Ko. Il s'agit du type de clé le plus courant. Il est utilisé pour protéger d'autres clés de données, telles que celles utilisées dans vos applications ou pour chiffrer les données en Services AWS votre nom.
- Clés asymétriques RSA ou à courbe elliptique : ces clés sont disponibles en différentes tailles et prennent en charge de nombreux algorithmes. Selon l'algorithme, ils peuvent être utilisés pour le chiffrement et le déchiffrement ainsi que pour les opérations de signature et de vérification.
- Clés symétriques pour effectuer des opérations de code d'authentification de message basé sur le hachage (HMAC) — Ces clés sont des clés de 256 bits utilisées pour les opérations de signature et de vérification.

Les clés KMS ne peuvent pas être exportées depuis le service en texte brut. Ils sont générés par et ne peuvent être utilisés que dans les modules de sécurité matériels (HSMs) utilisés par le service. Il s'agit d'une propriété de sécurité fondamentale destinée AWS KMS à empêcher la compromission des clés. Dans les régions de Chine (Pékin) et de Chine (Ningxia), HSMs ils sont certifiés par l'OSCCA. Dans toutes les autres régions, les données HSMs utilisées AWS KMS sont validées dans le cadre du programme FIPS 140 du NIST au niveau de sécurité 3. Pour plus d'informations sur la conception et les contrôles AWS KMS permettant de protéger vos clés, consultez la section Détails AWS Key Management Service cryptographiques.

Vous pouvez envoyer des données à l'aide AWS KMS de divers moyens cryptographiques APIs afin d'effectuer des opérations de chiffrement, de déchiffrement, de signature ou de vérification avec des clés KMS. Vous pouvez également choisir de faire en sorte qu'une clé KMS agisse comme une clé de chiffrement, qui protège un type de clé appelé clé de données. Une clé de données peut être exportée AWS KMS pour être utilisée dans votre application locale ou pour protéger les données en votre nom. Service AWS L'utilisation de clés de données est courante dans tous les systèmes de gestion de clés et est souvent appelée chiffrement d'enveloppes. Le chiffrement par enveloppe permet d'utiliser une clé de données sur le système distant qui gère vos données sensibles, au lieu

d'avoir à envoyer vos données sensibles AWS KMS pour qu'elles soient chiffrées directement sous une clé KMS.

Pour plus d'informations, consultez la section AWS KMS keyset les éléments essentiels de AWS KMS la cryptographie dans la AWS KMS documentation.

Bonnes pratiques de gestion clés pour AWS KMS

Lorsque vous utilisez AWS Key Management Service (AWS KMS), vous devez prendre certaines décisions de conception fondamentales. Il s'agit notamment de savoir s'il faut utiliser un modèle centralisé ou décentralisé pour la gestion des clés et l'accès, le type de clés à utiliser et le type de magasin de clés à utiliser. Les sections suivantes vous aident à prendre des décisions adaptées à votre organisation et à vos cas d'utilisation. Cette section se termine par des considérations importantes relatives à la désactivation et à la suppression des clés KMS, y compris les mesures que vous devez prendre pour protéger vos données et vos clés.

Cette section contient les rubriques suivantes :

- Choisir un modèle centralisé ou décentralisé
- Choix des clés gérées par le client, des clés AWS gérées ou des clés AWS détenues
- Choisir un magasin AWS KMS de clés
- Suppression et désactivation des clés KMS

Choisir un modèle centralisé ou décentralisé

AWS vous recommande d'utiliser plusieurs comptes Comptes AWS et de les gérer comme une seule organisation dans AWS Organizations. Il existe deux grandes approches de gestion AWS KMS keys dans les environnements multi-comptes.

La première approche est une approche décentralisée, dans laquelle vous créez des clés dans chaque compte qui utilise ces clés. Lorsque vous stockez les clés KMS dans les mêmes comptes que les ressources qu'elles protègent, il est plus facile de déléguer des autorisations aux administrateurs locaux qui comprennent les exigences d'accès relatives à leurs AWS principaux et à leurs clés. Vous pouvez autoriser l'utilisation des clés en utilisant simplement une politique clé, ou vous pouvez combiner une politique clé et des politiques basées sur l'identité dans AWS Identity and Access Management (IAM).

La deuxième approche est une approche centralisée, dans laquelle vous conservez les clés KMS dans une ou plusieurs clés désignées Comptes AWS. Vous autorisez les autres comptes à n'utiliser les clés que pour des opérations cryptographiques. Vous gérez les clés, leur cycle de vie et leurs autorisations à partir du compte centralisé. Vous autorisez d'autres Comptes AWS personnes à utiliser la clé, mais vous n'autorisez aucune autre autorisation. Les comptes externes ne peuvent rien

gérer concernant le cycle de vie de la clé ou les autorisations d'accès. Ce modèle centralisé permet de minimiser le risque de suppression involontaire de clés ou d'augmentation de privilèges par des administrateurs ou des utilisateurs délégués.

L'option que vous choisissez dépend de plusieurs facteurs. Tenez compte des points suivants lorsque vous choisissez une approche :

1. Disposez-vous d'un processus automatique ou manuel pour fournir l'accès aux clés et aux ressources ? Cela inclut des ressources telles que les pipelines de déploiement et les modèles d'infrastructure en tant que code (IaC). Ces outils peuvent vous aider à déployer et à gérer des ressources (telles que les clés KMS, les politiques clés, les rôles IAM et les politiques IAM) sur de nombreuses plateformes. Comptes AWS Si vous ne disposez pas de ces outils de déploiement, une approche centralisée de la gestion des clés peut être plus facile à gérer pour votre entreprise.
2. Disposez-vous d'un contrôle administratif sur tous ceux Comptes AWS qui contiennent des ressources utilisant des clés KMS ? Si tel est le cas, un modèle centralisé peut simplifier la gestion et éliminer le besoin de passer Comptes AWS à la gestion des clés. Notez toutefois que les rôles IAM et les autorisations utilisateur pour utiliser les clés doivent toujours être gérés par compte.
3. Devez-vous offrir l'accès à vos clés KMS à des clients ou à des partenaires qui disposent de leurs propres ressources Comptes AWS et de leurs propres ressources ? Pour ces clés, une approche centralisée peut réduire la charge administrative pesant sur vos clients et partenaires.
4. Avez-vous des exigences d'autorisation pour accéder aux AWS ressources qui sont mieux résolues par une approche d'accès centralisé ou local ? Par exemple, si différentes applications ou unités commerciales sont chargées de gérer la sécurité de leurs propres données, il est préférable d'adopter une approche décentralisée de la gestion des clés.
5. Dépassez-vous les quotas de ressources de service pour AWS KMS ? Comme ces quotas sont définis par Compte AWS, un modèle décentralisé répartit la charge entre les comptes, multipliant ainsi efficacement les quotas de service.

> **Note**
>
> Le modèle de gestion des clés n'est pas pertinent lorsque l'on considère les quotas de demande, car ces quotas sont appliqués au principal du compte qui fait une demande concernant la clé, et non au compte qui possède ou gère la clé.

En général, nous vous recommandons de commencer par une approche décentralisée, sauf si vous pouvez exprimer le besoin d'un modèle de clé KMS centralisé.

Choix des clés gérées par le client, des clés AWS gérées ou des clés AWS détenues

Les clés KMS que vous créez et gérez pour les utiliser dans vos propres applications cryptographiques sont appelées clés gérées par le client. Services AWS peut utiliser des clés gérées par le client pour chiffrer les données que le service stocke en votre nom. Les clés gérées par le client sont recommandées si vous souhaitez avoir un contrôle total sur le cycle de vie et l'utilisation de vos clés. L'ajout d'une clé gérée par le client à votre compte entraîne des frais mensuels. En outre, les demandes d'utilisation ou de gestion de la clé entraînent un coût d'utilisation. Pour en savoir plus, consultez Pricing AWS KMS (Tarification).

Si vous souhaitez chiffrer vos données sans avoir Service AWS à supporter les frais généraux ou les coûts liés à la gestion des clés, vous pouvez utiliser une cléAWS gérée. Ce type de clé existe dans votre compte, mais il ne peut être utilisé que dans certaines circonstances. Il ne peut être utilisé que dans le contexte de Service AWS celui dans lequel vous opérez, et il ne peut être utilisé que par les principaux utilisateurs du compte qui contient la clé. Vous ne pouvez rien gérer concernant le cycle de vie ou les autorisations de ces clés. Certains Services AWS utilisent des clés AWS gérées. Le format d'un alias de clé AWS gérée est`aws/<service code>`. Par exemple, une `aws/ebs` clé ne peut être utilisée que pour chiffrer les volumes Amazon Elastic Block Store (Amazon EBS) sur le même compte que la clé et ne peut être utilisée que par les responsables IAM de ce compte. Une clé AWS gérée ne peut être utilisée que par les utilisateurs de ce compte et pour les ressources de ce compte. Vous ne pouvez pas partager des ressources chiffrées sous une clé AWS gérée avec d'autres comptes. Si cela constitue une limite pour votre cas d'utilisation, nous vous recommandons d'utiliser plutôt une clé gérée par le client ; vous pouvez partager l'utilisation de cette clé avec n'importe quel autre compte. L'existence d'une clé AWS gérée sur votre compte ne vous est pas facturée, mais toute utilisation de ce type de clé par la personne assignée à la Service AWS clé vous est facturée.

Une clé AWS gérée est un ancien type de clé qui n'est plus créé pour une nouvelle clé à Services AWS partir de 2021. Au lieu de cela, les nouveaux (et Services AWS les anciens) AWS utilisent une clé propre pour chiffrer vos données par défaut. AWS les clés détenues sont un ensemble de clés KMS qu'un Service AWS utilisateur possède et gère pour une utilisation multiple Comptes AWS. Bien que ces clés ne se trouvent pas dans votre compte Compte AWS, un homme Service AWS peut en utiliser une pour protéger les ressources de votre compte.

Nous vous recommandons d'utiliser des clés gérées par le client lorsque le contrôle granulaire est le plus important et d'utiliser des clés AWS détenues lorsque la commodité est primordiale.

Le tableau suivant décrit les principales différences en matière de politique, de journalisation, de gestion et de tarification entre chaque type de clé. Pour plus d'informations sur les types de clés, consultez la section AWS KMS Concepts.

Considération	Clés gérées par le client	AWS clés gérées	AWS clés possédées
Stratégie de clé	Contrôlé exclusive ment par le client	Contrôlé par le service ; visible par le client	Contrôlé exclusive ment et uniquement visible par le système Service AWS qui crypte vos données
Journalisation	AWS CloudTrail suivi des clients ou magasin de données sur les événements	CloudTrail suivi des clients ou magasin de données sur les événements	Non visible par le client
Gestion du cycle de vie	Le client gère la rotation, la suppressi on et Région AWS	Service AWS gère la rotation (annuelle), la suppression et la région	Service AWS gère la rotation (annuelle), la suppression et la région
Tarification	Tarif mensuel pour l'existence de la clé (calculé au prorata de l'heure) ; l'utilisation de l'API est facturée à l'appelant	L'existence de la clé est gratuite ; l'utilisa tion de l'API est facturée à l'appelant	Aucuns frais pour le client

Choisir un magasin AWS KMS de clés

Un magasin de clés est un emplacement sécurisé pour le stockage et l'utilisation de clés cryptographiques. La meilleure pratique du secteur pour les magasins de clés consiste à utiliser un dispositif connu sous le nom de module de sécurité matériel (HSM) qui a été validé dans le cadre du programme de validation des modules cryptographiques FIPS (Federal Information Processing Standards) 140 du NIST au niveau de sécurité 3. Il existe d'autres programmes destinés à soutenir

les principaux magasins utilisés pour traiter les paiements. AWS Payment Cryptographyest un service que vous pouvez utiliser pour protéger les données relatives à vos charges de travail de paiement.

AWS KMS prend en charge plusieurs types de magasins de clés pour protéger vos informations clés lorsque vous AWS KMS les utilisez pour créer et gérer vos clés de chiffrement. Toutes les options de stockage de clés fournies par AWS KMS sont continuellement validées selon la norme FIPS 140 au niveau de sécurité 3. Ils sont conçus pour empêcher quiconque, y compris AWS les opérateurs, d'accéder à vos clés en texte brut ou de les utiliser sans votre autorisation. Pour plus d'informations sur les types de magasins de clés disponibles, consultez la section Magasins de clés de la AWS KMS documentation.

Le magasin de clés AWS KMS standard est le meilleur choix pour la majorité des charges de travail. Si vous devez choisir un autre type de magasin de clés, déterminez soigneusement si des exigences réglementaires ou autres (internes, par exemple) imposent ce choix, et évaluez soigneusement les coûts et les avantages.

Suppression et désactivation des clés KMS

La suppression d'une clé KMS peut avoir un impact significatif. Avant de supprimer une clé KMS que vous n'avez plus l'intention d'utiliser, déterminez s'il est approprié de définir l'état de la clé sur Désactivé. Lorsqu'une clé est désactivée, elle ne peut pas être utilisée pour des opérations cryptographiques. Il existe toujours dans AWS, et vous pourrez le réactiver à l'avenir si nécessaire. Les clés désactivées continuent d'entraîner des frais de stockage. Nous vous recommandons de désactiver les clés au lieu de les supprimer jusqu'à ce que vous soyez certain qu'elles ne protègent aucune donnée ou clé de données.

> **Important**
>
> La suppression d'une clé doit être soigneusement planifiée. Les données ne peuvent pas être déchiffrées si la clé correspondante a été supprimée. AWS n'a aucun moyen de récupérer une clé supprimée une fois qu'elle a été supprimée. Comme pour les autres opérations critiques AWS, vous devez appliquer une politique qui limite le nombre de personnes autorisées à planifier la suppression des clés et qui exige une authentification multifactorielle (MFA) pour la suppression des clés.

Pour éviter la suppression accidentelle de la clé, AWS KMS applique une période d'attente minimale par défaut de sept jours après l'exécution d'un `DeleteKey` appel avant de supprimer la clé. Vous pouvez fixer le délai d'attente à une valeur maximale de 30 jours. Pendant la période d'attente, la clé est toujours stockée AWS KMS dans un état en attente de suppression. Il ne peut pas être utilisé pour des opérations de chiffrement ou de déchiffrement. Toute tentative d'utilisation d'une clé dont l'état est en attente de suppression à des fins de chiffrement ou de déchiffrement est enregistrée. AWS CloudTrail Vous pouvez définir une CloudWatch alarme Amazon pour ces événements dans vos CloudTrail journaux. Si vous recevez des alertes concernant ces événements, vous pouvez choisir d'annuler le processus de suppression si nécessaire. Jusqu'à l'expiration du délai d'attente, vous pouvez récupérer la clé à partir de l'état En attente de suppression et la restaurer à l'état Désactivé ou Activé.

La suppression d'une clé multirégionale nécessite que vous supprimiez les répliques avant la copie d'origine. Pour plus d'informations, consultez la section Suppression de clés multirégionales.

Si vous utilisez une clé avec du matériel clé importé, vous pouvez supprimer le matériel clé importé immédiatement. Cela diffère de la suppression d'une clé KMS de plusieurs manières. Lorsque vous effectuez l'`DeleteImportedKeyMaterial`action, le contenu clé AWS KMS est supprimé et l'état de la clé passe à En attente d'importation. Une fois que vous avez supprimé le contenu de la clé, celle-ci devient immédiatement inutilisable. Il n'y a pas de période d'attente. Pour réactiver l'utilisation de la clé, vous devez réimporter le même matériel clé. La période d'attente pour la suppression des clés KMS s'applique également aux clés KMS contenant du matériel clé importé.

Si les clés de données sont protégées par une clé KMS et sont activement utilisées par Services AWS, elles ne sont pas immédiatement affectées si la clé KMS associée est désactivée ou si le contenu clé importé est supprimé. Supposons, par exemple, qu'une clé contenant du matériel importé ait été utilisée pour chiffrer un objet avec SSE-KMS. Vous êtes en train de télécharger l'objet dans un compartiment Amazon Simple Storage Service (Amazon S3). Avant de télécharger l'objet dans le compartiment, vous devez importer le contenu dans votre clé. Une fois l'objet chargé, vous supprimez le contenu clé importé de cette clé. L'objet reste chiffré dans le compartiment, mais personne ne peut y accéder tant que le contenu clé supprimé n'est pas réimporté dans la clé. Bien que ce flux nécessite une automatisation précise pour importer et supprimer des éléments clés d'une clé, il peut fournir un niveau de contrôle supplémentaire au sein d'un environnement.

AWS propose des conseils prescriptifs pour vous aider à surveiller et à corriger (si nécessaire) la suppression planifiée des clés KMS. Pour plus d'informations, voir Surveiller et corriger la suppression planifiée des AWS KMS clés.

Bonnes pratiques en matière de protection des données pour AWS KMS

Cette section vous aide à faire des choix concernant l'utilisation des clés AWS Key Management Service (AWS KMS) pour la protection des données, telles que les clés à utiliser pour chaque type de données. Il fournit également des exemples spécifiques d'utilisation AWS KMS avec différents Services AWS. Ces recommandations et exemples vous aident à comprendre le nombre de clés dont vous pourriez avoir besoin et les principaux qui ont besoin d'autorisations pour utiliser ces clés.

La section traite également de la rotation des clés. La rotation des clés consiste soit à remplacer une clé KMS existante par une nouvelle clé, soit à remplacer le matériel cryptographique associé à une clé KMS existante par du nouveau matériel. Ce guide fournit des exemples et des instructions expliquant comment faire pivoter les clés KMS pour un usage courant Services AWS. Les recommandations et les exemples sont conçus pour vous aider à faire des choix éclairés concernant votre principale stratégie de rotation.

Enfin, cette section fournit des recommandations sur la façon d'utiliser l' AWS Encryption SDK outil permettant d'implémenter le chiffrement côté client dans vos applications. Cette section inclut les choix de conception que vous pouvez effectuer en fonction de l'ensemble des fonctionnalités et des capacités du AWS Encryption SDK.

Cette section aborde les sujets de chiffrement suivants :

- Chiffrement avec AWS KMS
- Rotation clé AWS KMS et portée de l'impact
- Recommandations pour l'utilisation du AWS Encryption SDK

Chiffrement avec AWS KMS

Le chiffrement est une bonne pratique générale pour protéger la confidentialité et l'intégrité des informations sensibles. Vous devez utiliser vos niveaux de classification de données existants et disposer d'au moins une AWS Key Management Service (AWS KMS) clé par niveau. Par exemple, vous pouvez définir une clé KMS pour les données classées comme confidentielles, une clé pour les données internes uniquement et une pour les données sensibles. Cela vous permet de vous assurer que seuls les utilisateurs autorisés sont autorisés à utiliser les clés associées à chaque niveau de classification.

> **Note**
>
> Une clé KMS unique gérée par le client peut être utilisée dans n'importe quelle combinaison d'applications Services AWS ou dans vos propres applications stockant des données d'une classification particulière. Le facteur limitant lié à l'utilisation d'une clé pour plusieurs charges de travail réside dans la complexité des autorisations d'utilisation nécessaires pour contrôler l'accès aux données d'un ensemble d'utilisateurs. Services AWS Le document JSON de politique AWS KMS clé doit être inférieur à 32 Ko. Si cette restriction de taille devient une limitation, envisagez d'utiliser AWS KMS des autorisations ou de créer plusieurs clés afin de minimiser la taille du document de politique clé.

Au lieu de vous fier uniquement à la classification des données pour partitionner votre clé KMS, vous pouvez également choisir d'attribuer une clé KMS à utiliser pour une classification des données au sein d'une seule clé Service AWS. Par exemple, toutes les données étiquetées `Sensitive` dans Amazon Simple Storage Service (Amazon S3) doivent être chiffrées sous une clé KMS portant un nom tel que. `S3-Sensitive` Vous pouvez également répartir vos données sur plusieurs clés KMS au sein de votre classification de données Service AWS et/ou de votre application définies. Par exemple, vous pouvez peut-être supprimer certains ensembles de données au cours d'une période donnée et en supprimer d'autres au cours d'une autre période. Vous pouvez utiliser des balises de ressources pour identifier et trier les données chiffrées à l'aide de clés KMS spécifiques.

Si vous optez pour un modèle de gestion décentralisé pour les clés KMS, vous devez appliquer des garde-fous pour vous assurer que de nouvelles ressources avec une classification donnée sont créées et utiliser les clés KMS attendues avec les autorisations appropriées. Pour plus d'informations sur la manière dont vous pouvez appliquer, détecter et gérer la configuration des ressources à l'aide de l'automatisation, consultez la Détection et surveillance section de ce guide.

Cette section aborde les sujets de chiffrement suivants :

- Chiffrement des données du journal avec AWS KMS
- Chiffrement par défaut
- Cryptage de base de données avec AWS KMS
- Chiffrement des données PCI DSS avec AWS KMS
- Utilisation de clés KMS avec Amazon EC2 Auto Scaling

Chiffrement des données du journal avec AWS KMS

Beaucoup Services AWS, comme Amazon GuardDuty et Amazon AWS CloudTrail, proposent des options pour chiffrer les données de journal envoyées à Amazon S3. Lorsque vous exportez GuardDuty des résultats depuis Amazon S3, vous devez utiliser une clé KMS. Nous vous recommandons de chiffrer toutes les données du journal et de n'accorder l'accès au déchiffrement qu'aux personnes autorisées, telles que les équipes de sécurité, les intervenants en cas d'incident et les auditeurs.

L'architecture AWS de référence de sécurité recommande de créer une centrale Compte AWS pour la journalisation. Ce faisant, vous pouvez également réduire vos frais de gestion des clés. Par exemple, avec CloudTrail, vous pouvez créer un journal d'organisation ou un magasin de données d'événements pour enregistrer les événements au sein de votre organisation. Lorsque vous configurez le magasin de données de suivi ou d'événement de votre organisation, vous pouvez spécifier un seul compartiment Amazon S3 et une seule clé KMS dans le compte de journalisation que vous avez désigné. Cette configuration s'applique à tous les comptes membres de l'organisation. Tous les comptes envoient ensuite leurs CloudTrail journaux au compartiment Amazon S3 du compte de journalisation, et les données des journaux sont chiffrées avec la clé KMS spécifiée. Vous devez mettre à jour la politique de clé pour cette clé KMS afin d'accorder CloudTrail les autorisations nécessaires pour utiliser la clé. Pour plus d'informations, consultez la section Configurer les politiques AWS KMS clés pour CloudTrail dans la CloudTrail documentation.

Pour protéger les CloudTrail journaux GuardDuty et, le compartiment Amazon S3 et la clé KMS doivent se trouver dans le même emplacement Région AWS. L'architecture AWS de référence de sécurité fournit également des conseils sur la journalisation et les architectures multi-comptes. Lorsque vous regroupez des journaux entre plusieurs régions et comptes, consultez la section Création d'un journal pour une organisation dans la CloudTrail documentation pour en savoir plus sur les régions optionnelles et vous assurer que votre journalisation centralisée fonctionne comme prévu.

Chiffrement par défaut

Services AWS qui stockent ou traitent des données offrent généralement un chiffrement au repos. Cette fonctionnalité de sécurité permet de protéger vos données en les chiffrant lorsqu'elles ne sont pas utilisées. Les utilisateurs autorisés peuvent toujours y accéder en cas de besoin.

Les options de mise en œuvre et de chiffrement varient entre les deux Services AWS. Beaucoup proposent le chiffrement par défaut. Il est important de comprendre le fonctionnement du chiffrement pour chaque service que vous utilisez. Voici quelques exemples :

- Amazon Elastic Block Store (Amazon EBS) — Lorsque vous activez le chiffrement par défaut, tous les nouveaux volumes et copies instantanées Amazon EBS sont chiffrés. AWS Identity and Access Management Les rôles ou utilisateurs (IAM) ne peuvent pas lancer d'instances avec des volumes non chiffrés ou des volumes qui ne prennent pas en charge le chiffrement. Cette fonctionnalité contribue à la sécurité, à la conformité et à l'audit en garantissant que toutes les données stockées sur les volumes Amazon EBS sont chiffrées. Pour plus d'informations sur le chiffrement dans ce service, consultez le chiffrement Amazon EBS dans la documentation Amazon EBS.
- Amazon Simple Storage Service (Amazon S3) — Tous les nouveaux objets sont chiffrés par défaut. Amazon S3 applique automatiquement le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) pour chaque nouvel objet, sauf si vous spécifiez une option de chiffrement différente. Les responsables IAM peuvent toujours charger des objets non chiffrés sur Amazon S3 en le mentionnant explicitement dans l'appel d'API. Dans Amazon S3, pour appliquer le chiffrement SSE-KMS, vous devez utiliser une politique de compartiment comportant des conditions qui nécessitent le chiffrement. Pour un exemple de politique, consultez Exiger SSE-KMS pour tous les objets écrits dans un compartiment dans la documentation Amazon S3. Certains compartiments Amazon S3 reçoivent et servent un grand nombre d'objets. Si ces objets sont chiffrés à l'aide de clés KMS, un grand nombre d'opérations Amazon S3 se traduisent par un grand nombre d'`Decrypt`appels `GenerateDataKey` et d'appels à AWS KMS. Cela peut augmenter les frais d' AWS KMS utilisation que vous devez payer. Vous pouvez configurer les clés de compartiment Amazon S3, ce qui peut réduire considérablement vos AWS KMS coûts. Pour plus d'informations sur le chiffrement dans ce service, consultez la section Protection des données par le chiffrement dans la documentation Amazon S3.
- Amazon DynamoDB — DynamoDB est un service de base de données NoSQL entièrement géré qui permet le chiffrement au repos côté serveur par défaut, et vous ne pouvez pas le désactiver. Nous vous recommandons d'utiliser une clé gérée par le client pour chiffrer vos tables DynamoDB. Cette approche vous permet de mettre en œuvre le principe du moindre privilège avec des autorisations granulaires et une séparation des tâches en ciblant des utilisateurs et des rôles IAM spécifiques dans vos politiques AWS KMS clés. Vous pouvez également choisir des clés AWS gérées ou AWS détenues lors de la configuration des paramètres de chiffrement pour vos tables DynamoDB. Pour les données nécessitant un degré élevé de protection (où les données ne doivent être visibles que sous forme de texte clair pour le client), envisagez d'utiliser le chiffrement côté client avec le SDK de chiffrement de AWS base de données. Pour plus d'informations sur le chiffrement de ce service, consultez la section Protection des données dans la documentation DynamoDB.

Cryptage de base de données avec AWS KMS

Le niveau auquel vous implémentez le chiffrement affecte les fonctionnalités de la base de données. Voici les compromis que vous devez prendre en compte :

- Si vous utilisez uniquement le AWS KMS chiffrement, le stockage qui sauvegarde vos tables est chiffré pour DynamoDB et Amazon Relational Database Service (Amazon RDS). Cela signifie que le système d'exploitation qui exécute la base de données voit le contenu du stockage en texte clair. Toutes les fonctions de base de données, y compris la génération d'index et les autres fonctions d'ordre supérieur qui nécessitent un accès aux données en texte clair, continuent de fonctionner comme prévu.
- Amazon RDS repose sur le chiffrement Amazon Elastic Block Store (Amazon EBS) pour assurer le chiffrement intégral des volumes de base de données. Lorsque vous créez une instance de base de données chiffrée avec Amazon RDS, Amazon RDS crée un volume Amazon EBS chiffré en votre nom pour stocker la base de données. Les données stockées au repos sur le volume, les instantanés de base de données, les sauvegardes automatisées et les répliques de lecture sont tous chiffrés sous la clé KMS que vous avez spécifiée lors de la création de l'instance de base de données.
- Amazon Redshift s'intègre AWS KMS et crée une hiérarchie de clés à quatre niveaux qui sont utilisées pour chiffrer le niveau du cluster via le niveau des données. Lorsque vous lancez votre cluster, vous pouvez choisir d'utiliser AWS KMS le chiffrement. Seuls l'application Amazon Redshift et les utilisateurs disposant des autorisations appropriées peuvent voir le texte en clair lorsque les tables sont ouvertes (et déchiffrées) en mémoire. Ceci est globalement analogue aux fonctionnalités de chiffrement des données transparentes ou basées sur des tables (TDE) disponibles dans certaines bases de données commerciales. Cela signifie que toutes les fonctions de base de données, y compris la génération d'index et les autres fonctions d'ordre supérieur qui nécessitent un accès aux données en texte clair, continuent de fonctionner comme prévu.
- Le chiffrement des données côté client mis en œuvre par le biais du SDK de chiffrement AWS de base de données (et d'outils similaires) signifie que le système d'exploitation et la base de données ne voient que le texte chiffré. Les utilisateurs peuvent afficher du texte clair uniquement s'ils accèdent à la base de données à partir d'un client sur lequel le SDK AWS de chiffrement de base de données est installé et s'ils ont accès à la clé appropriée. Les fonctions de base de données d'ordre supérieur qui nécessitent l'accès au texte clair pour fonctionner comme prévu, telles que la génération d'index, ne fonctionneront pas si on leur demande d'opérer sur des champs chiffrés. Lorsque vous choisissez d'utiliser le chiffrement côté client, assurez-vous d'utiliser un mécanisme de chiffrement robuste qui aide à prévenir les attaques courantes contre les données chiffrées.

Cela inclut l'utilisation d'un algorithme de chiffrement puissant et de techniques appropriées, telles qu'un sel, pour aider à atténuer les attaques par texte chiffré.

Nous recommandons d'utiliser les fonctionnalités de chiffrement AWS KMS intégrées pour les services AWS de base de données. Pour les charges de travail qui traitent des données sensibles, le chiffrement côté client doit être envisagé pour les champs de données sensibles. Lorsque vous utilisez le chiffrement côté client, vous devez tenir compte de l'impact sur l'accès à la base de données, comme les jointures dans les requêtes SQL ou la création d'index.

Chiffrement des données PCI DSS avec AWS KMS

Les contrôles de sécurité et de qualité AWS KMS ont été validés et certifiés conformément aux exigences de la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS). Cela signifie que vous pouvez chiffrer les données du numéro de compte principal (PAN) à l'aide d'une clé KMS. L'utilisation d'une clé KMS pour chiffrer les données élimine une partie de la charge de gestion des bibliothèques de chiffrement. En outre, les clés KMS ne peuvent pas être exportées AWS KMS, ce qui réduit les risques de stockage non sécurisé des clés de chiffrement.

Vous pouvez utiliser d'autres méthodes AWS KMS pour répondre aux exigences de la norme PCI DSS. Par exemple, si vous utilisez AWS KMS Amazon S3, vous pouvez stocker les données PAN dans Amazon S3 car le mécanisme de contrôle d'accès de chaque service est distinct de l'autre.

Comme toujours, lorsque vous examinez vos exigences de conformité, assurez-vous d'obtenir des conseils auprès de parties dûment expérimentées, qualifiées et vérifiées. Tenez compte des quotas de AWS KMS demandes lorsque vous concevez des applications qui utilisent directement la clé pour protéger les données de transaction par carte relevant du champ d'application de la norme PCI DSS.

Toutes les AWS KMS demandes étant enregistrées AWS CloudTrail, vous pouvez vérifier l'utilisation des clés en consultant les CloudTrail journaux. Toutefois, si vous utilisez des clés de compartiment Amazon S3, aucune entrée ne correspond à chaque action Amazon S3. Cela est dû au fait que la clé de compartiment chiffre les clés de données que vous utilisez pour chiffrer les objets dans Amazon S3. Bien que l'utilisation d'une clé de compartiment n'élimine pas tous les appels d'API AWS KMS, elle en réduit le nombre. Par conséquent, il n'y a plus de one-to-one correspondance entre les tentatives d'accès aux objets Amazon S3 et les appels d'API à AWS KMS.

Utilisation de clés KMS avec Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling est un service recommandé pour automatiser le dimensionnement de vos EC2 instances Amazon. Cela vous permet de vous assurer que vous disposez du nombre correct

d'instances disponibles pour gérer la charge de votre application. Amazon EC2 Auto Scaling utilise un rôle lié au service qui fournit les autorisations appropriées au service et autorise ses activités au sein de votre compte. Pour utiliser les clés KMS avec Amazon EC2 Auto Scaling, vos politiques AWS KMS clés doivent autoriser le rôle lié au service à utiliser votre clé KMS pour certaines opérations d'API`Decrypt`, par exemple pour que l'automatisation soit utile. Si la politique AWS KMS clé n'autorise pas le principal IAM qui effectue l'opération à effectuer une action, cette action sera refusée. Pour plus d'informations sur la manière d'appliquer correctement les autorisations dans la politique clé pour autoriser l'accès, consultez la section Protection des données dans Amazon EC2 Auto Scaling dans la documentation Amazon EC2 Auto Scaling.

Rotation clé AWS KMS et portée de l'impact

Nous ne recommandons pas AWS Key Management Service (AWS KMS) la rotation des clés, sauf si vous êtes obligé de faire pivoter les clés pour des raisons de conformité réglementaire. Par exemple, il se peut que vous deviez effectuer une rotation de vos clés KMS en raison de politiques commerciales, de règles contractuelles ou de réglementations gouvernementales. La conception de réduit AWS KMS considérablement les types de risques que la rotation des clés est généralement utilisée pour atténuer. Si vous devez faire pivoter les touches KMS, nous vous recommandons d'utiliser la rotation automatique des touches et de n'utiliser la rotation manuelle des touches que si la rotation automatique des touches n'est pas prise en charge.

Cette section aborde les principaux sujets suivants relatifs à la rotation :

- AWS KMS rotation symétrique des clés
- Rotation clé pour les volumes Amazon EBS
- Rotation des clés pour Amazon RDS
- Rotation clé pour Amazon S3 et la réplication dans la même région
- Clés KMS rotatives avec matériel importé

AWS KMS rotation symétrique des clés

AWS KMS prend en charge la rotation automatique des clés uniquement pour les clés KMS de chiffrement symétriques dont le contenu clé est AWS KMS créé. La rotation automatique est facultative pour les clés KMS gérées par le client. Sur une base annuelle, AWS KMS alterne le matériel clé pour les clés KMS AWS gérées. AWS KMS enregistre toutes les versions précédentes du matériel cryptographique à perpétuité, afin que vous puissiez déchiffrer toutes les données chiffrées avec cette clé KMS. AWS KMS ne supprime aucun élément clé pivoté tant que vous n'avez

pas supprimé la clé KMS. En outre, lorsque vous déchiffrez un objet en utilisant AWS KMS, le service détermine le support approprié à utiliser pour l'opération de déchiffrement ; aucun paramètre d'entrée supplémentaire ne doit être fourni.

Étant donné AWS KMS que les versions précédentes des clés cryptographiques sont conservées et que vous pouvez utiliser ces informations pour déchiffrer les données, la rotation des clés n'apporte aucun avantage supplémentaire en termes de sécurité. Le mécanisme de rotation des clés existe pour faciliter la rotation des clés si vous gérez une charge de travail dans un contexte où des exigences réglementaires ou autres l'exigent.

Rotation clé pour les volumes Amazon EBS

Vous pouvez faire pivoter les clés de données Amazon Elastic Block Store (Amazon EBS) en utilisant l'une des approches suivantes. L'approche dépend de vos flux de travail, de vos méthodes de déploiement et de l'architecture de votre application. Cela peut être utile lorsque vous passez d'une clé AWS gérée à une clé gérée par le client.

Pour utiliser les outils du système d'exploitation pour copier les données d'un volume à un autre

1. Créez la nouvelle clé KMS. Pour obtenir des instructions, reportez-vous à la section Création d'une clé KMS.
2. Créez un nouveau volume Amazon EBS dont la taille est identique ou supérieure à celle de l'original. Pour le chiffrement, spécifiez la clé KMS que vous avez créée. Pour obtenir des instructions, consultez la section Créer un volume Amazon EBS.
3. Montez le nouveau volume sur la même instance ou le même conteneur que le volume d'origine. Pour obtenir des instructions, consultez Attacher un volume Amazon EBS à une EC2 instance Amazon.
4. À l'aide de l'outil de votre système d'exploitation préféré, copiez les données du volume existant vers le nouveau volume.
5. Lorsque la synchronisation est terminée, pendant une fenêtre de maintenance préplanifiée, arrêtez le trafic vers l'instance. Pour obtenir des instructions, consultez la section Arrêter et démarrer manuellement vos instances.
6. Démontez le volume d'origine. Pour obtenir des instructions, consultez Détacher un volume Amazon EBS d'une instance Amazon EC2 .
7. Montez le nouveau volume sur le point de montage d'origine.
8. Vérifiez que le nouveau volume fonctionne correctement.

9. Supprimez le volume d'origine. Pour obtenir des instructions, consultez Supprimer un volume Amazon EBS.

Pour utiliser un instantané Amazon EBS pour copier les données d'un volume à un autre

1. Créez la nouvelle clé KMS. Pour obtenir des instructions, reportez-vous à la section Création d'une clé KMS.
2. Créez un instantané Amazon EBS du volume d'origine. Pour obtenir des instructions, consultez la section Créer des instantanés Amazon EBS.
3. Créez un volume à partir de l'instantané. Pour le chiffrement, spécifiez la nouvelle clé KMS que vous avez créée. Pour obtenir des instructions, consultez la section Créer un volume Amazon EBS.

   > **Note**
   >
   > En fonction de votre charge de travail, vous souhaiterez peut-être utiliser la restauration rapide des instantanés Amazon EBS afin de minimiser la latence initiale sur le volume.

4. Créez une nouvelle EC2 instance Amazon. Pour obtenir des instructions, consultez Lancer une EC2 instance Amazon.
5. Attachez le volume que vous avez créé à l' EC2 instance Amazon. Pour obtenir des instructions, consultez Attacher un volume Amazon EBS à une EC2 instance Amazon.
6. Faites passer la nouvelle instance en production.
7. Faites pivoter l'instance d'origine hors production et supprimez-la. Pour obtenir des instructions, consultez Supprimer un volume Amazon EBS.

> **Note**
>
> Il est possible de copier des instantanés et de modifier la clé de chiffrement utilisée pour la copie cible. Après avoir copié l'instantané et l'avoir chiffré avec vos clés KMS préférées, vous pouvez également créer une Amazon Machine Image (AMI) à partir des instantanés. Pour plus d'informations, consultez la section Chiffrement Amazon EBS dans la EC2 documentation Amazon.

Rotation des clés pour Amazon RDS

Pour certains services, tels qu'Amazon Relational Database Service (Amazon RDS), le chiffrement des données est effectué au sein du service et est fourni par. AWS KMS Suivez les instructions suivantes pour faire pivoter une clé pour une instance de base de données Amazon RDS.

Pour faire pivoter une clé KMS pour une base de données Amazon RDS

1. Créez un instantané de la base de données cryptée d'origine. Pour obtenir des instructions, consultez la section Gestion des sauvegardes manuelles dans la documentation Amazon RDS.
2. Copiez le cliché dans un nouvel instantané. Pour le chiffrement, spécifiez la nouvelle clé KMS. Pour obtenir des instructions, consultez Copier un instantané de base de données pour Amazon RDS.
3. Utilisez le nouvel instantané pour créer un nouveau cluster Amazon RDS. Pour obtenir des instructions, consultez la section Restauration vers une instance de base de données dans la documentation Amazon RDS. Par défaut, le cluster utilise la nouvelle clé KMS.
4. Vérifiez le fonctionnement de la nouvelle base de données et des données qu'elle contient.
5. Faites passer la nouvelle base de données en production.
6. Faites pivoter l'ancienne base de données hors production et supprimez-la. Pour obtenir des instructions, consultez Supprimer une instance de base de données.

Rotation clé pour Amazon S3 et la réplication dans la même région

Pour Amazon Simple Storage Service (Amazon S3), pour modifier la clé de chiffrement d'un objet, vous devez lire et réécrire l'objet. Lorsque vous réécrivez l'objet, vous spécifiez explicitement la nouvelle clé de chiffrement lors de l'opération d'écriture. Pour ce faire, vous pouvez utiliser Amazon S3 Batch Operations pour de nombreux objets. Dans les paramètres de la tâche, pour l'opération de copie, spécifiez les nouveaux paramètres de chiffrement. Par exemple, vous pouvez choisir SSE-KMS et saisir le KeyID.

Vous pouvez également utiliser Amazon S3 Same-Replication (SRR). Le SSR peut rechiffrer les objets en transit.

Clés KMS rotatives avec matériel importé

AWS KMS ne récupère ni ne fait pivoter votre matériel clé importé. Pour faire pivoter une clé KMS avec du matériel clé importé, vous devez faire pivoter la clé manuellement.

Recommandations pour l'utilisation du AWS Encryption SDK

AWS Encryption SDKIl s'agit d'un outil puissant pour implémenter le chiffrement côté client dans vos applications. Des bibliothèques sont disponibles pour Java JavaScript, C, Python et d'autres langages de programmation. Il s'intègre à AWS Key Management Service (AWS KMS). Vous pouvez également l'utiliser en tant que SDK autonome sans faire référence aux clés KMS.

Les pratiques recommandées pour l'utilisation de cet outil incluent une prise en compte attentive des exigences de votre application. Équilibrez ces exigences par rapport aux risques pouvant être introduits par certaines configurations, tels que l'introduction de la mise en cache des clés dans votre application. Pour plus d'informations sur la mise en cache des clés de données, consultez la section Mise en cache des clés de données dans la AWS Encryption SDK documentation.

Tenez compte des questions suivantes pour déterminer s'il convient d'utiliser AWS Encryption SDK :

- Existe-t-il une exigence de chiffrement côté client qui ne peut pas être satisfaite par le chiffrement côté serveur avec des services intégrés ? AWS KMS
- Pouvez-vous protéger de manière adéquate les clés utilisées pour chiffrer les données côté client, et comment allez-vous vous y prendre ?
- Existe-t-il d'autres bibliothèques de fit-for-purpose chiffrement qui pourraient mieux répondre à votre cas d'utilisation ? Envisagez d'autres AWS offres, telles que le chiffrement côté client Amazon S3 et le SDK de chiffrement des AWS bases de données.

Pour plus d'informations sur le choix du service adapté à votre cas d'utilisation, consultez la documentation de AWS Crypto Tools.

Bonnes pratiques de gestion des identités et des accès pour AWS KMS

Pour utiliser AWS Key Management Service (AWS KMS), vous devez disposer d'informations d'identification AWS permettant d'authentifier et d'autoriser vos demandes. Aucun AWS principal n'a d'autorisation sur une clé KMS à moins que cette autorisation ne soit fournie explicitement et ne soit jamais refusée. Il n'existe aucune autorisation implicite ou automatique pour utiliser ou gérer une clé KMS. Les rubriques de cette section définissent les meilleures pratiques en matière de sécurité afin de vous aider à déterminer les contrôles de gestion des AWS KMS accès à utiliser pour sécuriser votre infrastructure.

Cette section aborde les sujets suivants relatifs à la gestion des identités et des accès :

- AWS KMS politiques clés et politiques IAM
- Autorisations du moindre privilège pour AWS KMS
- Contrôle d'accès basé sur les rôles pour AWS KMS
- Contrôle d'accès basé sur les attributs pour AWS KMS
- Contexte de chiffrement pour AWS KMS
- AWS KMS Permissions de dépannage

AWS KMS politiques clés et politiques IAM

Les politiques constituent le principal moyen de gérer l'accès à vos AWS KMS ressources. Les politiques sont des documents qui décrivent quels principaux peuvent accéder à quelles ressources. Les politiques associées à une identité AWS Identity and Access Management (IAM) (utilisateurs, groupes d'utilisateurs ou rôles) sont appelées politiques basées sur l'identité. Les politiques IAM associées aux ressources sont appelées politiques basées sur les ressources. AWS KMS les politiques de ressources pour les clés KMS sont appelées politiques clés. Outre les politiques IAM et les politiques AWS KMS clés, AWS KMS soutient les subventions. Les subventions constituent un moyen flexible et puissant de déléguer des autorisations. Vous pouvez utiliser des subventions pour délivrer un accès par clé KMS limité dans le temps aux principaux IAM de votre entreprise Compte AWS ou d'une autre entreprise. Comptes AWS

Toutes les clés KMS ont une politique de clé. Si vous n'en fournissez pas, AWS KMS créez-en un pour vous. La politique de clé par défaut AWS KMS utilisée varie selon que vous créez la clé à l'aide

de la AWS KMS console ou de l' AWS KMS API. Nous vous recommandons de modifier la politique clé par défaut afin de l'aligner sur les exigences de votre organisation en matière d'autorisations du moindre privilège. Cela doit également correspondre à votre stratégie d'utilisation des politiques IAM en conjonction avec des politiques clés. Pour plus de recommandations sur l'utilisation des politiques IAM avec AWS KMS, consultez la section Meilleures pratiques relatives aux politiques IAM dans la AWS KMS documentation.

Vous pouvez utiliser la politique clé pour déléguer l'autorisation d'un principal IAM à la politique basée sur l'identité. Vous pouvez également utiliser la politique clé pour affiner l'autorisation en conjonction avec la politique basée sur l'identité. Dans les deux cas, la politique clé et la politique basée sur l'identité déterminent l'accès, ainsi que toute autre politique applicable qui délimite l'accès, telle que les politiques de contrôle des services (SCPs), les politiques de contrôle des ressources (RCPs) ou les limites d'autorisation. Si le principal se trouve sur un compte différent de celui de la clé KMS, seules les actions cryptographiques et de subvention sont prises en charge. Pour plus d'informations sur ce scénario multi-comptes, voir Autoriser les utilisateurs d'autres comptes à utiliser une clé KMS dans la AWS KMS documentation.

Vous devez utiliser des politiques basées sur l'identité IAM en combinaison avec des politiques clés pour contrôler l'accès à vos clés KMS. Les autorisations peuvent également être utilisées en combinaison avec ces politiques pour contrôler l'accès à une clé KMS. Pour utiliser une politique basée sur l'identité afin de contrôler l'accès à une clé KMS, la politique de clé doit autoriser le compte à utiliser des politiques basées sur l'identité. Vous pouvez soit spécifier une déclaration de politique clé qui active les politiques IAM, soit spécifier explicitement les principes autorisés dans la politique clé.

Lorsque vous rédigez des politiques, assurez-vous de disposer de contrôles stricts qui limitent les personnes autorisées à effectuer les actions suivantes :

- Mettre à jour, créer et supprimer les politiques IAM et les politiques clés KMS
- Associer et détacher les politiques basées sur l'identité des utilisateurs, des rôles et des groupes
- Attacher et détacher les politiques AWS KMS clés des clés KMS
- Créez des autorisations pour vos clés KMS : que vous contrôliez l'accès à vos clés KMS exclusivement à l'aide de politiques clés ou que vous combiniez des politiques clés avec des politiques IAM, vous devez limiter la possibilité de modifier les politiques. Mettez en œuvre un processus d'approbation pour modifier les politiques existantes. Un processus d'approbation peut aider à éviter ce qui suit :

- Perte accidentelle des autorisations principales IAM — Il est possible d'apporter des modifications qui empêcheraient les administrateurs IAM de gérer la clé ou de l'utiliser dans le cadre d'opérations cryptographiques. Dans des scénarios extrêmes, il est possible de révoquer les autorisations de gestion des clés de tous les utilisateurs. Dans ce cas, vous devez nous contacter AWS Supportpour retrouver l'accès à la clé.
- Modifications non approuvées des politiques clés KMS : si un utilisateur non autorisé accède à la politique clé, il peut la modifier pour déléguer des autorisations à un utilisateur involontaire Compte AWS ou principal.
- Modifications non approuvées des politiques IAM — Si un utilisateur non autorisé obtient un ensemble d'informations d'identification avec les autorisations nécessaires pour gérer les membres d'un groupe, il peut augmenter ses propres autorisations et apporter des modifications à vos politiques IAM, politiques clés, configuration des clés KMS ou autres configurations de ressources. AWS

Passez en revue attentivement les rôles et les utilisateurs IAM associés aux principaux IAM désignés comme vos administrateurs de clés KMS. Cela peut aider à empêcher les suppressions ou modifications non autorisées. Si vous devez modifier les principaux qui ont accès à vos clés KMS, vérifiez que les nouveaux administrateurs principaux sont ajoutés à toutes les politiques clés requises. Testez leurs autorisations avant de supprimer l'ancien directeur général. Nous vous recommandons vivement de suivre toutes les meilleures pratiques de sécurité IAM et d'utiliser des informations d'identification temporaires plutôt que des informations d'identification à long terme.

Nous vous recommandons de délivrer un accès limité dans le temps par le biais de subventions si vous ne connaissez pas le nom des principaux au moment de la création des politiques ou si les principaux nécessitant un accès changent fréquemment. Le principal du bénéficiaire peut être sur le même compte que la clé KMS ou sur un autre compte. Si le principal et la clé KMS se trouvent dans des comptes différents, vous devez spécifier une politique basée sur l'identité en plus de l'autorisation. Les subventions nécessitent une gestion supplémentaire, car vous devez appeler une API pour créer la subvention et pour retirer ou révoquer l'autorisation lorsqu'elle n'est plus nécessaire.

Aucun AWS principal, y compris l'utilisateur root du compte ou le créateur de la clé, n'est autorisé à accéder à une clé KMS à moins qu'il ne soit explicitement autorisé et non explicitement refusé dans une politique clé, une politique IAM ou une subvention. Par extension, vous devez envisager ce qui se passerait si un utilisateur obtenait un accès involontaire pour utiliser une clé KMS et quel en serait l'impact. Pour atténuer un tel risque, considérez les points suivants :

- Vous pouvez gérer différentes clés KMS pour différentes catégories de données. Cela vous permet de séparer les clés et de maintenir des politiques clés plus concises contenant des déclarations de politique ciblant spécifiquement l'accès principal à cette catégorie de données. Cela signifie également que si les informations d'identification IAM pertinentes sont consultées par inadvertance, l'identité liée à cet accès n'a accès qu'aux clés spécifiées dans la politique IAM et uniquement si la politique en matière de clés autorise l'accès à ce principal.
- Vous pouvez évaluer si un utilisateur ayant un accès involontaire à la clé peut accéder aux données. Par exemple, avec Amazon Simple Storage Service (Amazon S3), l'utilisateur doit également disposer des autorisations appropriées pour accéder aux objets chiffrés dans Amazon S3. Par ailleurs, si un utilisateur a un accès involontaire (via RDP ou SSH) à une EC2 instance Amazon dont le volume est chiffré à l'aide d'une clé KMS, il peut accéder aux données à l'aide des outils du système d'exploitation.

> **Note**
>
> Services AWS qui utilisent AWS KMS n'exposent pas le texte chiffré aux utilisateurs (la plupart des approches actuelles de cryptoanalyse nécessitent l'accès au texte chiffré). En outre, le texte chiffré n'est pas disponible pour examen physique en dehors d'un centre de AWS données car tous les supports de stockage sont physiquement détruits lors de leur mise hors service, conformément aux exigences NIST 00-88. SP8

Autorisations du moindre privilège pour AWS KMS

Étant donné que vos clés KMS protègent les informations sensibles, nous vous recommandons de suivre le principe de l'accès le moins privilégié. Déléguez les autorisations minimales requises pour effectuer une tâche lorsque vous définissez vos politiques clés. N'autorisez toutes les actions (`kms:*`) sur une politique de clé KMS que si vous prévoyez de restreindre davantage les autorisations avec des politiques supplémentaires basées sur l'identité. Si vous envisagez de gérer les autorisations à l'aide de politiques basées sur l'identité, limitez le nombre de personnes habilitées à créer des politiques IAM et à les associer à des principes IAM, et surveillez les modifications apportées aux politiques.

Si vous autorisez toutes les actions (`kms:*`) à la fois dans la politique clé et dans la politique basée sur l'identité, le principal dispose des autorisations d'administration et d'utilisation de la clé KMS. Pour des raisons de sécurité, nous vous recommandons de déléguer ces autorisations uniquement

à des responsables spécifiques. Réfléchissez à la manière dont vous attribuez des autorisations aux principaux qui géreront vos clés et aux principaux qui utiliseront vos clés. Vous pouvez le faire en nommant explicitement le principal dans la politique clé ou en limitant les principes auxquels la politique basée sur l'identité est attachée. Vous pouvez également utiliser des clés de condition pour restreindre les autorisations. Par exemple, vous pouvez utiliser aws : PrincipalTag pour autoriser toutes les actions si le principal effectuant l'appel d'API possède la balise spécifiée dans la règle de condition.

Pour mieux comprendre comment les déclarations de politique sont évaluées AWS, consultez la section Logique d'évaluation des politiques dans la documentation IAM. Nous vous recommandons de consulter cette rubrique avant de rédiger des politiques afin de réduire le risque que votre politique ait des effets imprévus, tels que l'octroi d'un accès à des mandants qui ne devraient pas y avoir accès.

> **Tip**
>
> Lorsque vous testez une application dans un environnement hors production, utilisez AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) pour vous aider à appliquer les autorisations du moindre privilège dans vos politiques IAM.

Si vous utilisez des utilisateurs IAM plutôt que des rôles IAM, nous vous recommandons vivement d'utiliser l'authentification AWS multifactorielle (MFA) pour atténuer la vulnérabilité des informations d'identification à long terme. Vous pouvez utiliser MFA pour effectuer les tâches suivantes :

- Exigez que les utilisateurs valident leurs informations d'identification auprès de la MFA avant d'effectuer des actions privilégiées, telles que la planification de la suppression de clés.
- Répartissez la propriété du mot de passe d'un compte administrateur et du dispositif MFA entre les individus afin de mettre en œuvre une autorisation partagée.

Pour des exemples de politiques qui peuvent vous aider à configurer les autorisations de moindre privilège, consultez les exemples de politiques IAM dans la documentation. AWS KMS

Contrôle d'accès basé sur les rôles pour AWS KMS

Le contrôle d'accès basé sur les rôles (RBAC) est une stratégie d'autorisation qui fournit aux utilisateurs uniquement les autorisations nécessaires pour effectuer leurs tâches, et rien de plus. C'est une approche qui peut vous aider à mettre en œuvre le principe du moindre privilège.

AWS KMS prend en charge le RBAC. Il vous permet de contrôler l'accès à vos clés en spécifiant des autorisations détaillées dans le cadre des politiques clés. Les politiques clés spécifient une ressource, une action, un effet, un principal et des conditions facultatives pour accorder l'accès aux clés. Pour implémenter le RBAC dans AWS KMS, nous recommandons de séparer les autorisations pour les utilisateurs clés et les administrateurs principaux.

Pour les utilisateurs clés, attribuez uniquement les autorisations dont ils ont besoin. Posez les questions suivantes pour affiner davantage les autorisations :

- Quels sont les responsables IAM qui ont besoin d'accéder à la clé ?
- Quelles actions chaque directeur doit-il effectuer avec la clé ? Par exemple, le directeur a-t-il uniquement besoin d'`Sign`autorisations `Encrypt` et d'autorisations ?
- À quelles ressources le directeur doit-il accéder ?
- L'entité est-elle un être humain ou un Service AWS ? S'il s'agit d'un service, vous pouvez utiliser la clé de ViaService condition kms : pour limiter l'utilisation des clés à un service spécifique.

Pour les administrateurs principaux, attribuez uniquement les autorisations dont l'administrateur a besoin. Par exemple, les autorisations d'un administrateur peuvent varier selon que la clé est utilisée dans des environnements de test ou de production. Si vous utilisez des autorisations moins restrictives dans certains environnements hors production, implémentez un processus pour tester les politiques avant leur mise en production.

Pour des exemples de politiques qui peuvent vous aider à configurer le contrôle d'accès basé sur les rôles pour les principaux utilisateurs et administrateurs, voir RBAC pour. AWS KMS

Contrôle d'accès basé sur les attributs pour AWS KMS

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs. Comme le RBAC, il s'agit d'une approche qui peut vous aider à mettre en œuvre le principe du moindre privilège.

AWS KMS prend en charge l'ABAC en vous permettant de définir des autorisations en fonction des balises associées à la ressource cible, telles qu'une clé KMS, et des balises associées au principal effectuant l'appel d'API. Dans AWS KMS, vous pouvez utiliser des balises et des alias pour contrôler l'accès aux clés gérées par vos clients. Par exemple, vous pouvez définir des politiques IAM qui utilisent des clés de condition de balise pour autoriser les opérations lorsque la balise du principal

correspond à la balise associée à la clé KMS. Pour un didacticiel, voir Définir les autorisations d'accès aux AWS ressources en fonction des balises de la AWS KMS documentation.

La meilleure pratique consiste à utiliser les stratégies ABAC pour simplifier la gestion des politiques IAM. Avec ABAC, les administrateurs peuvent utiliser des balises pour autoriser l'accès à de nouvelles ressources au lieu de mettre à jour les politiques existantes. ABAC nécessite moins de politiques, car il n'est pas nécessaire de créer des politiques différentes pour les différentes fonctions professionnelles. Pour plus d'informations, consultez la section Comparaison entre ABAC et le modèle RBAC traditionnel dans la documentation IAM.

Appliquez les meilleures pratiques en matière d'autorisations de moindre privilège au modèle ABAC. Fournissez aux responsables IAM uniquement les autorisations dont ils ont besoin pour effectuer leur travail. Contrôlez soigneusement l'accès au balisage APIs qui permettrait aux utilisateurs de modifier les balises associées aux rôles et aux ressources. Si vous utilisez des clés de condition d'alias de clé pour prendre en charge l'ABAC dans AWS KMS, assurez-vous de disposer également de contrôles stricts qui limitent les personnes autorisées à créer des clés et à modifier des alias.

Vous pouvez également utiliser des balises pour associer une clé spécifique à une catégorie d'entreprise et vérifier que la bonne clé est utilisée pour une action donnée. Par exemple, vous pouvez utiliser AWS CloudTrail les journaux pour vérifier que la clé utilisée pour effectuer une AWS KMS action spécifique appartient à la même catégorie professionnelle que la ressource sur laquelle elle est utilisée.

> ⚠ Warning
>
> N'incluez pas d'informations confidentielles ou sensibles dans la clé de balise ou la valeur de balise. Les tags ne sont pas chiffrés. Ils sont accessibles à de nombreuses personnes Services AWS, y compris la facturation.

Avant de mettre en œuvre une approche ABAC pour votre contrôle d'accès, déterminez si les autres services que vous utilisez prennent en charge cette approche. Pour savoir quels services sont compatibles avec ABAC, consultez la documentation relative àServices AWS l'utilisation d'ABAC dans la documentation IAM.

Pour plus d'informations sur la mise en œuvre d'ABAC pour AWS KMS et les clés de conditions qui peuvent vous aider à configurer les politiques, consultez ABAC pour. AWS KMS

Contexte de chiffrement pour AWS KMS

Toutes les opérations AWS KMS cryptographiques utilisant des clés KMS de chiffrement symétriques acceptent un contexte de chiffrement. Le contexte de chiffrement est un ensemble facultatif de paires clé-valeur non secrètes qui peuvent contenir des informations contextuelles supplémentaires sur les données. La meilleure pratique consiste à insérer un contexte de chiffrement dans les `Encrypt` opérations AWS KMS afin d'améliorer l'autorisation et l'auditabilité de vos appels d'API de déchiffrement à. AWS KMS AWS KMS utilise le contexte de chiffrement en tant que données authentifiées supplémentaires (AAD) pour prendre en charge le chiffrement authentifié. Le contexte de chiffrement est lié cryptographiquement au texte chiffré, de sorte que le même contexte de chiffrement est requis pour déchiffrer les données.

Le contexte de chiffrement n'est pas secret ou chiffré. Il apparaît en texte clair dans AWS CloudTrail les journaux afin que vous puissiez l'utiliser pour identifier et classer vos opérations cryptographiques. Le contexte de chiffrement n'étant pas secret, vous ne devez autoriser que les principaux autorisés à accéder aux données de vos CloudTrail journaux.

Vous pouvez également utiliser les clés de condition kms ::context-key EncryptionContext et kms : pour contrôler l'accès à une EncryptionContextKeys clé KMS de chiffrement symétrique en fonction du contexte de chiffrement. Vous pouvez également utiliser ces clés de condition pour exiger que des contextes de chiffrement soient utilisés dans les opérations cryptographiques. Pour ces clés de condition, consultez les instructions relatives à l'utilisation `ForAnyValue` ou à la `ForAllValues` définition des opérateurs afin de vous assurer que vos politiques reflètent les autorisations que vous souhaitez obtenir.

AWS KMS Permissions de dépannage

Lorsque vous rédigez des politiques de contrôle d'accès pour une clé KMS, réfléchissez à la manière dont la stratégie IAM et la politique clé fonctionnent ensemble. Les autorisations effectives pour un directeur sont celles qui sont accordées (et non refusées explicitement) par toutes les politiques en vigueur. Au sein d'un compte, les autorisations relatives à une clé KMS peuvent être affectées par les politiques basées sur l'identité IAM, les politiques clés, les limites des autorisations, les politiques de contrôle des services ou les politiques de session. Par exemple, si vous utilisez à la fois des politiques basées sur l'identité et des clés pour contrôler l'accès à la clé KMS, toutes les politiques relatives au principal et à la ressource sont évaluées afin de déterminer l'autorisation du principal à effectuer une action donnée. Pour plus d'informations, consultez la section Logique d'évaluation des politiques dans la documentation IAM.

Pour obtenir des informations détaillées et un organigramme permettant de résoudre les problèmes d'accès par clé, consultez la section Résolution des problèmes d'accès par clé dans la AWS KMS documentation.

Pour résoudre un message d'erreur de refus d'accès

1. Vérifiez que les politiques basées sur l'identité IAM et les politiques clés KMS autorisent l'accès.
2. Vérifiez qu'une limite d'autorisations dans IAM ne restreint pas l'accès.
3. Vérifiez qu'une politique de contrôle des services (SCP) ou une politique de contrôle des ressources (RCP) ne restreint pas l'accès. AWS Organizations
4. Si vous utilisez des points de terminaison VPC, vérifiez que les politiques de point de terminaison sont correctes.
5. Dans les politiques basées sur l'identité et les politiques clés, supprimez toutes les conditions ou références aux ressources qui limitent l'accès à la clé. Après avoir supprimé ces restrictions, vérifiez que le principal peut appeler avec succès l'API qui a échoué précédemment. En cas de succès, réappliquez les conditions et les références aux ressources une par une, puis vérifiez que le principal y a toujours accès. Cela vous permet d'identifier la condition ou la référence de ressource à l'origine de l'erreur.

Pour plus d'informations, consultez la section Résolution des messages d'erreur liés au refus d'accès dans la documentation IAM.

Bonnes pratiques de détection et de surveillance pour AWS KMS

La détection et la surveillance jouent un rôle important dans la compréhension de la disponibilité, de l'état et de l'utilisation de vos AWS Key Management Service (AWS KMS) clés. La surveillance permet de maintenir la sécurité, la fiabilité, la disponibilité et les performances de vos AWS solutions. AWS fournit plusieurs outils pour surveiller vos clés et vos AWS KMS opérations KMS. Cette section décrit comment configurer et utiliser ces outils pour obtenir une meilleure visibilité sur votre environnement et surveiller l'utilisation de vos clés KMS.

Cette section aborde les sujets de détection et de surveillance suivants :

- Surveillance AWS KMS des opérations avec AWS CloudTrail
- Surveillance de l'accès aux clés KMS avec IAM Access Analyzer
- Surveillance des paramètres de chiffrement d'autres utilisateurs Services AWS avec AWS Config
- Surveillance des clés KMS avec les CloudWatch alarmes Amazon
- Automatiser les réponses avec Amazon EventBridge

Surveillance AWS KMS des opérations avec AWS CloudTrail

AWS KMS est intégré à AWS CloudTrailun service qui peut enregistrer tous les appels AWS KMS adressés par les utilisateurs, les rôles, Services AWS etc. CloudTrail capture tous les appels d'API AWS KMS sous forme d'événements, y compris les appels provenant de la AWS KMS console AWS KMS APIs AWS CloudFormation,,, the AWS Command Line Interface (AWS CLI) et Outils AWS pour PowerShell.

CloudTrail enregistre toutes les AWS KMS opérations, y compris les opérations en lecture seule, telles `ListAliases` que et. `GetKeyRotationStatus` Il enregistre également les opérations qui gèrent les clés KMS, telles que `CreateKey` et `PutKeyPolicy, and cryptographic operations, such as GenerateDataKey` et`Decrypt`. Il enregistre également les opérations internes AWS KMS qui vous concernent, telles que `DeleteExpiredKeyMaterial``DeleteKey`,`SynchronizeMultiRegionKey`, et`RotateKey`.

CloudTrail est activé sur votre ordinateur Compte AWS lorsque vous le créez. Par défaut, l'historique des événements fournit un enregistrement consultable, consultable, téléchargeable et immuable

des 90 derniers jours d'activité d'API de gestion des événements enregistrés dans un. Région AWS Pour surveiller ou auditer l'utilisation de vos clés KMS au-delà de cette période de 90 jours, nous vous recommandons de créer une CloudTrail trace pour votre compte Compte AWS. Si vous avez créé une organisation dans AWS Organizations, vous pouvez créer un journal d'organisation ou un magasin de données d'événements qui enregistre les événements pour tous Comptes AWS les membres de cette organisation.

Une fois que vous avez établi un suivi pour votre compte ou votre organisation, vous pouvez en Services AWS utiliser d'autres pour stocker, analyser et répondre automatiquement aux événements enregistrés dans le suivi. Par exemple, vous pouvez effectuer les opérations suivantes :

- Vous pouvez configurer des CloudWatch alarmes Amazon qui vous avertissent de certains événements survenus pendant le parcours. Pour plus d'informations, consultez

  > Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez l'utiliser CloudWatch pour collecter et suivre les métriques, qui sont des variables que vous pouvez mesurer.
  >
  > L'expiration de documents clés importés ou la suppression d'une clé sont des événements potentiellement catastrophiques s'ils ne sont pas intentionnels ou s'ils ne sont pas correctement planifiés. Nous vous recommandons de configurer des CloudWatch alarmes pour vous avertir de ces événements avant qu'ils ne se produisent. Nous vous recommandons également de configurer des politiques AWS Identity and Access Management (IAM) ou des politiques de contrôle des AWS Organizations services (SCPs) pour empêcher la suppression de clés importantes.
  >
  > CloudWatch les alarmes vous aident à prendre des mesures correctives, telles que l'annulation de la suppression des clés, ou des actions correctives, telles que la réimportation des éléments clés supprimés ou expirés.

  dans ce guide.
- Vous pouvez créer des EventBridge règles Amazon qui exécutent automatiquement une action lorsqu'un événement se produit dans le parcours. Pour plus d'informations, consultez Automatiser les réponses avec Amazon EventBridge dans ce guide.
- Vous pouvez utiliser Amazon Security Lake pour collecter et stocker des journaux provenant de plusieurs sites Services AWS, notamment CloudTrail. Pour plus d'informations, consultez la section Collecte de données depuis Services AWS Security Lake dans la documentation Amazon Security Lake.

- Pour améliorer votre analyse de l'activité opérationnelle, vous pouvez interroger CloudTrail les journaux avec Amazon Athena. Pour plus d'informations, consultez les AWS CloudTrail journaux de requêtes dans la documentation Amazon Athena.

Pour plus d'informations sur la surveillance AWS KMS des opérations avec CloudTrail, consultez les rubriques suivantes :

- Journalisation des appels d' AWS KMS API avec AWS CloudTrail
- Exemples d'entrées de AWS KMS journal
- Surveillez les clés KMS avec Amazon EventBridge
- CloudTrail intégration avec Amazon EventBridge

Surveillance de l'accès aux clés KMS avec IAM Access Analyzer

AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) vous aide à identifier les ressources de votre organisation et les comptes (tels que les clés KMS) partagés avec une entité externe. Ce service peut vous aider à identifier les accès involontaires ou trop étendus à vos ressources et à vos données, ce qui constitue un risque pour la sécurité. IAM Access Analyzer identifie les ressources partagées avec des acteurs externes en utilisant un raisonnement basé sur la logique pour analyser les politiques basées sur les ressources dans votre environnement. AWS

Vous pouvez utiliser IAM Access Analyzer pour identifier les entités externes qui ont accès à vos clés KMS. Lorsque vous activez IAM Access Analyzer, vous créez un analyseur pour l'ensemble d'une organisation ou pour un compte cible. L'organisation ou le compte que vous choisissez est connu sous le nom de zone de confiance de l'analyseur. L'analyseur surveille les ressources prises en charge dans la zone de confiance. Tout accès aux ressources par des mandants se trouvant dans la zone de confiance est considéré comme fiable.

Pour les clés KMS, IAM Access Analyzer analyse les politiques clés et les autorisations appliquées à une clé. Il permet de déterminer si une politique ou une autorisation de clé permet à une entité externe d'accéder à la clé. Utilisez IAM Access Analyzer pour déterminer si des entités externes ont accès à vos clés KMS, puis vérifiez si ces entités doivent y avoir accès.

Pour plus d'informations sur l'utilisation d'IAM Access Analyzer pour surveiller l'accès par clé KMS, consultez les rubriques suivantes :

- Utilisation de AWS Identity and Access Management Access Analyzer

- Types de ressources IAM Access Analyzer pour accès externe
- Types de ressources IAM Access Analyzer : AWS KMS keys
- Résultats relatifs à l'accès externe et non utilisé

Surveillance des paramètres de chiffrement d'autres utilisateurs Services AWS avec AWS Config

AWS Configfournit une vue détaillée de la configuration des AWS ressources de votre Compte AWS. Vous pouvez l'utiliser AWS Config pour vérifier Services AWS que les paramètres de chiffrement des utilisateurs de vos clés KMS sont correctement configurés. Par exemple, vous pouvez utiliser la AWS Config règle des volumes cryptés pour vérifier que vos volumes Amazon Elastic Block Store (Amazon EBS) sont chiffrés.

AWS Config inclut des règles gérées qui vous aident à choisir rapidement les règles par rapport auxquelles évaluer vos ressources. Vérifiez AWS Config si Régions AWS les règles gérées dont vous avez besoin sont prises en charge dans cette région. Les règles gérées disponibles incluent la vérification de la configuration des instantanés Amazon Relational Database Service (Amazon RDS), le chiffrement des traces CloudTrail , le chiffrement par défaut pour les compartiments Amazon Simple Storage Service (Amazon S3), le chiffrement des tables Amazon DynamoDB, etc.

Vous pouvez également créer des règles personnalisées et appliquer votre logique métier pour déterminer si vos ressources sont conformes à vos exigences. Le code open source de nombreuses règles gérées est disponible dans le référentiel de AWS Config règles sur GitHub. Elles peuvent constituer un point de départ utile pour développer vos propres règles personnalisées.

Lorsqu'une ressource n'est pas conforme à une règle, vous pouvez lancer des actions réactives. AWS Config inclut les actions correctives mises en œuvre par AWS Systems Manager Automation. Par exemple, si vous avez appliqué la cloud-trail-encryption-enabledrègle et que celle-ci renvoie un `NON_COMPLIANT` résultat, vous AWS Config pouvez créer un document d'automatisation qui résout le problème en chiffrant les CloudTrail journaux pour vous.

AWS Config vous permet de vérifier de manière proactive le respect des AWS Config règles avant de provisionner des ressources. L'application de règles en mode proactif vous permet d'évaluer les configurations de vos ressources cloud avant leur création ou leur mise à jour. L'application de règles en mode proactif dans le cadre de votre pipeline de déploiement vous permet de tester les configurations des ressources avant de les déployer.

Vous pouvez également implémenter AWS Config des règles sous forme de contrôles AWS Security Hub. Security Hub propose des normes de sécurité que vous pouvez appliquer à votre Comptes AWS. Ces normes vous aident à évaluer votre environnement par rapport aux pratiques recommandées. La norme des meilleures pratiques de sécuritéAWS fondamentales inclut des contrôles relevant de la catégorie de contrôle de protection pour vérifier que le chiffrement au repos est configuré et que les politiques clés KMS respectent les pratiques recommandées.

Pour plus d'informations sur l'utilisation AWS Config pour surveiller les paramètres de chiffrement dans Services AWS, consultez les rubriques suivantes :

- Démarrer avec AWS Config
- AWS Config règles gérées
- AWS Config règles personnalisées
- Corriger les ressources non conformes avec AWS Config

Surveillance des clés KMS avec les CloudWatch alarmes Amazon

Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez l'utiliser CloudWatch pour collecter et suivre les métriques, qui sont des variables que vous pouvez mesurer.

L'expiration de documents clés importés ou la suppression d'une clé sont des événements potentiellement catastrophiques s'ils ne sont pas intentionnels ou s'ils ne sont pas correctement planifiés. Nous vous recommandons de configurer des CloudWatch alarmes pour vous avertir de ces événements avant qu'ils ne se produisent. Nous vous recommandons également de configurer des politiques AWS Identity and Access Management (IAM) ou des politiques de contrôle des AWS Organizations services (SCPs) pour empêcher la suppression de clés importantes.

CloudWatch les alarmes vous aident à prendre des mesures correctives, telles que l'annulation de la suppression des clés, ou des actions correctives, telles que la réimportation des éléments clés supprimés ou expirés.

Automatiser les réponses avec Amazon EventBridge

Vous pouvez également utiliser Amazon EventBridge pour vous informer des événements importants qui affectent vos clés KMS. EventBridge est un système Service AWS qui fournit un flux en temps quasi réel d'événements système décrivant les modifications apportées aux AWS ressources.

EventBridgereçoit automatiquement les événements CloudTrail de Security Hub. Dans EventBridge, vous pouvez créer des règles qui répondent aux événements enregistrés par CloudTrail.

AWS KMS les événements incluent les suivants :

- Le matériau clé d'une clé KMS a été automatiquement pivoté
- Le contenu clé importé d'une clé KMS a expiré
- Une clé KMS dont la suppression avait été planifiée a été supprimée

Ces événements peuvent déclencher des actions supplémentaires dans votre Compte AWS. Ces actions sont différentes des CloudWatch alarmes décrites dans la section précédente car elles ne peuvent être mises en œuvre qu'après la survenue de l'événement. Par exemple, vous souhaiterez peut-être supprimer des ressources connectées à une clé spécifique après la suppression de cette clé, ou vous souhaiterez peut-être informer une équipe de conformité ou d'audit que la clé a été supprimée.

Vous pouvez également filtrer tout autre événement d'API connecté en CloudTrail utilisant EventBridge. Cela signifie que si les principales actions d'API liées aux politiques sont particulièrement préoccupantes, vous pouvez les filtrer. Par exemple, vous pouvez filtrer EventBridge pour l'action d'`PutKeyPolicy`API. De manière plus générale, vous pouvez filtrer toute action d'API qui commence par `Disable*` ou `Delete*` pour lancer des réponses automatisées.

En utilisant EventBridge, vous pouvez surveiller (qui est un contrôle de détection), enquêter et réagir (qui sont des contrôles réactifs) à des événements inattendus ou sélectionnés. Par exemple, vous pouvez alerter les équipes de sécurité et prendre des mesures spécifiques si un utilisateur ou un rôle IAM est créé, lorsqu'une clé KMS est créée ou lorsqu'une politique clé est modifiée. Vous pouvez créer une règle d' EventBridge événement qui filtre les actions d'API que vous spécifiez, puis associez des cibles à la règle. Les exemples de cibles incluent AWS Lambda les fonctions, les notifications Amazon Simple Notification Service (Amazon SNS), les files d'attente Amazon Simple Queue Service (Amazon SQS), etc. Pour plus d'informations sur l'envoi d'événements à des cibles, consultez la section Cibles du bus d'événements sur Amazon EventBridge.

Pour plus d'informations sur la surveillance AWS KMS EventBridge et l'automatisation des réponses, consultez la section Surveiller les clés KMS avec Amazon EventBridge dans la AWS KMS documentation.

Bonnes pratiques de gestion des coûts et de la facturation pour AWS KMS

Grâce à l'ampleur et à la profondeur, Services AWS offrez la flexibilité nécessaire pour gérer vos coûts tout en répondant aux exigences de l'entreprise. Cette section traite de la tarification du stockage des clés dans AWS Key Management Service (AWS KMS) et fournit des recommandations pour réduire les coûts, par exemple grâce à la mise en cache des clés. Vous pouvez également examiner l'utilisation des clés KMS afin de déterminer s'il existe d'autres possibilités de réduire les coûts.

Cette section aborde les sujets suivants relatifs à la gestion des coûts et de la facturation :

- AWS KMS tarification du stockage des clés
- Clés de compartiment Amazon S3 avec chiffrement par défaut
- Mise en cache des clés de données à l'aide du AWS Encryption SDK
- Alternatives à la mise en cache des clés et aux clés de compartiment Amazon S3
- Gestion des coûts de journalisation liés à l'utilisation des clés KMS

AWS KMS tarification du stockage des clés

Chaque création dans AWS KMS key laquelle vous créez AWS KMS entraîne des frais. Les frais mensuels sont les mêmes pour les clés symétriques, les clés asymétriques, les clés HMAC, les clés multirégionales (chaque clé principale et chaque réplique de clé multirégionale), les clés dont le contenu clé est importé et les clés KMS dont l'origine provient d'une banque de clés externe AWS CloudHSM ou d'une banque de clés externe.

Pour les clés KMS que vous faites pivoter automatiquement ou à la demande, la première et la deuxième rotation de la clé entraînent des frais mensuels supplémentaires (calculés au prorata de l'heure). Après la deuxième rotation, les rotations suivantes au cours de ce mois ne sont pas facturées. Veuillez consulter les AWS KMS tarifs pour obtenir les dernières informations sur les prix.

Vous pouvez l'utiliser AWS Budgetspour configurer un budget d'utilisation. AWS Budgets peut vous avertir lorsque les dépenses de votre compte dépassent certains seuils. Pour les coûts associés AWS KMS, vous pouvez créer un budget d'utilisation pour émettre des alertes en fonction des clés ou des demandes KMS. Cela peut améliorer votre visibilité sur le stockage de vos AWS KMS clés et les coûts d'utilisation.

Clés de compartiment Amazon S3 avec chiffrement par défaut

Dans certains cas d'utilisation, les charges de travail qui accèdent à un grand nombre d'objets ou en génèrent un grand nombre dans Amazon Simple Storage Service (Amazon S3) peuvent générer d'importants volumes de demandes, ce qui AWS KMS augmente vos coûts. La configuration des clés de compartiment Amazon S3 peut vous aider à réduire les coûts jusqu'à 99 %. Il s'agit d'une alternative recommandée à la désactivation du chiffrement afin de réduire les coûts associés AWS KMSà.

Mise en cache des clés de données à l'aide du AWS Encryption SDK

Lorsque vous utilisez le AWS Encryption SDKpour effectuer un chiffrement côté client, la mise en cache des clés de données peut contribuer à améliorer les performances de votre application, à réduire le risque de limitation des demandes de votre application et à réduire AWS KMS les coûts. Pour plus d'informations sur la façon de démarrer, voir Comment utiliser la mise en cache des clés de données.

Alternatives à la mise en cache des clés et aux clés de compartiment Amazon S3

Si la mise en cache des clés n'est pas une option pour vous en raison de vos exigences en matière de traitement des données, vous pouvez également demander des augmentations de AWS KMS quotas en utilisant l'API AWS Management Console ou l'API Service Quotas. Tenez compte du volume d'appels d'API que vous pourriez effectuer. Le nombre d'appels d'API que vous effectuez est un facteur important dans la AWS KMS tarification. Si vous augmentez le quota de taux de demandes pour améliorer vos performances, le nombre croissant de demandes AWS KMS entraîne des coûts supplémentaires.

Gestion des coûts de journalisation liés à l'utilisation des clés KMS

Tous les appels d' AWS KMS API sont enregistrés dans AWS CloudTrail. Les applications et les services peuvent générer de gros volumes d'appels d' AWS KMS API (par exemple pour les opérations cryptographiques, y compris le chiffrement et le déchiffrement). Il peut être difficile de consulter CloudTrail les journaux sans un outil qui vous aide à organiser ces données, à étudier les

tendances et à rechercher les activités anormales des API. Amazon Athena fournit des structures de données prédéfinies qui peuvent vous aider à configurer rapidement des tables pour les CloudTrail journaux et à commencer à analyser les données de vos journaux. Il est particulièrement utile pour une analyse ad hoc ou une enquête plus approfondie lors de la réponse à un incident. Pour plus d'informations, consultez la section AWS CloudTrail Journaux des requêtes dans la documentation d'Athena.

Comme vous payez pour Athena par requête, vous pouvez configurer vos tables à l'avance sans frais. Les déclarations relatives à la langue de définition des données ne sont pas facturées. Lorsque vous répondez à un incident, cela vous permet de vous assurer que de nombreuses conditions préalables sont déjà remplies. Pour vous aider à vous préparer, il est recommandé d'écrire vos requêtes après avoir créé votre table, de les tester et de vous assurer qu'elles produisent les résultats souhaités. Vous pouvez enregistrer vos requêtes dans Athena pour une utilisation future. Pour plus d'informations sur la façon de démarrer avec Athena, consultez Getting started with Amazon Athena.

Les événements de données fournissent une visibilité sur les opérations effectuées sur ou au sein d'une ressource. Ils sont également connus sous le nom opérations de plans de données. Les exemples incluent les `PutObject` événements Amazon S3 ou les appels d'API pour le fonctionnement de la fonction Lambda. Les événements liés aux données sont souvent des activités à volume élevé, et leur enregistrement entraîne des frais. Pour aider à contrôler le volume d'événements de données enregistrés dans les pistes ou les données d'événements stockées CloudTrail, vous pouvez optimiser votre journalisation afin de réduire les coûts pour CloudTrail AWS KMS, et Amazon S3 en configurant des sélecteurs d'événements avancés afin de limiter les événements de données auxquels vous devez vous connecter CloudTrail. Pour plus d'informations, voir Comment optimiser AWS CloudTrail les coûts à l'aide de sélecteurs d'événements avancés (article de AWS blog).

Ressources

AWS Key Management Service (AWS KMS) documentation

- AWS KMS Manuel du développeur
- Référence d'API AWS KMS
- AWS KMS dans la AWS CLI référence

Outils

- AWS Encryption SDK

AWS Conseils prescriptifs

Politiques

- Création d'une stratégie de chiffrement pour les données au repos

Guides

- Meilleures pratiques et fonctionnalités de chiffrement pour Services AWS
- AWS Architecture de référence en matière de confidentialité (AWS PRA)

Modèles

- Chiffrez automatiquement les volumes Amazon EBS
- Corriger automatiquement les instances et clusters de base de données Amazon RDS non chiffrés
- Surveillez et corrigez la suppression planifiée de AWS KMS keys

Collaborateurs

Conception

- Frank Phillis, architecte de solutions spécialisé senior GTM, AWS
- Ken Beer, directeur AWS KMS des bibliothèques cryptographiques, AWS
- Michael Miller, architecte de solutions senior, AWS
- Jeremy Stieglitz, chef de produit principal, AWS
- Zach Miller, architecte de solutions principal, AWS
- Peter M. O'Donnell, architecte principal des solutions, AWS
- Patrick Palmer, architecte de solutions principal, AWS
- Dave Walker, architecte principal des solutions, AWS

Révision

- Manigandan Shri, consultant principal en livraison, AWS

Rédaction technique

- Lilly AbouHarb, rédactrice technique senior, AWS
- Kimberly Garmoe, rédactrice technique principale, AWS

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	—	24 mars 2025

AWS Glossaire des directives prescriptives

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

Nombres

7 R

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

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

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

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

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

migration active-passive

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

fonction d'agrégation

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

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

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

anti-motif

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

contrôle des applications

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

portefeuille d'applications

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

intelligence artificielle (IA)

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

opérations d'intelligence artificielle (AIOps)

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

chiffrement asymétrique

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

atomicité, cohérence, isolement, durabilité (ACID)

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

contrôle d'accès par attributs (ABAC)

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

source de données faisant autorité

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

Zone de disponibilité

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

AWS Cadre d'adoption du cloud (AWS CAF)

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

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

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

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

B

mauvais bot

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

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

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

système de poids fort

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

classification binaire

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

filtre de Bloom

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

déploiement bleu/vert

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

bot

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

botnet

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

branche

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

accès par brise-vitre

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

stratégie existante (brownfield)

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

cache de tampon

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

capacité métier

Ce que fait une entreprise pour générer de la valeur (par exemple, les ventes, le service client ou le marketing). Les architectures de microservices et les décisions de développement

peuvent être dictées par les capacités métier. Pour plus d'informations, veuillez consulter la section Organisation en fonction des capacités métier du livre blanc Exécution de microservices conteneurisés sur AWS.

planification de la continuité des activités (BCP)

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

C

CAF

Voir le cadre d'adoption du AWS cloud.

déploiement de Canary

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

CCo E

Voir le Centre d'excellence du cloud.

CDC

Voir capture des données de modification.

capture des données de modification (CDC)

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

ingénierie du chaos

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

CI/CD

Découvrez l'intégration continue et la livraison continue.

classification

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

chiffrement côté client

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

Centre d'excellence du cloud (CCoE)

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

cloud computing

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

modèle d'exploitation du cloud

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

étapes d'adoption du cloud

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

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

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

CMDB

Voir base de données de gestion de configuration.

référentiel de code

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

cache passif

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

données gelées

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

vision par ordinateur (CV)

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

dérive de configuration

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

base de données de gestion des configurations (CMDB)

Référentiel qui stocke et gère les informations relatives à une base de données et à son environnement informatique, y compris les composants matériels et logiciels ainsi que leurs

configurations. Vous utilisez généralement les données d'une CMDB lors de la phase de découverte et d'analyse du portefeuille de la migration.

pack de conformité

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

intégration continue et livraison continue (CI/CD)

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

CV

Voir vision par ordinateur.

D

données au repos

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

classification des données

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

dérive des données

Une variation significative entre les données de production et les données utilisées pour entraîner un modèle ML, ou une modification significative des données d'entrée au fil du temps. La dérive

des données peut réduire la qualité, la précision et l'équité globales des prédictions des modèles ML.

données en transit

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

maillage de données

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

minimisation des données

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

périmètre de données

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

prétraitement des données

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

provenance des données

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

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

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

langage de définition de base de données (DDL)

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

langage de manipulation de base de données (DML)

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

DDL

Voir langage de définition de base de données.

ensemble profond

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

deep learning

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

defense-in-depth

Approche de la sécurité de l'information dans laquelle une série de mécanismes et de contrôles de sécurité sont judicieusement répartis sur l'ensemble d'un réseau informatique afin de protéger la confidentialité, l'intégrité et la disponibilité du réseau et des données qu'il contient. Lorsque vous adoptez cette stratégie AWS, vous ajoutez plusieurs contrôles à différentes couches de la AWS Organizations structure afin de sécuriser les ressources. Par exemple, une defense-in-depth approche peut combiner l'authentification multifactorielle, la segmentation du réseau et le chiffrement.

administrateur délégué

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

déploiement

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

environnement de développement

Voir environnement.

contrôle de détection

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

cartographie de la chaîne de valeur du développement (DVSM)

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

jumeau numérique

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

tableau des dimensions

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

catastrophe

Un événement qui empêche une charge de travail ou un système d'atteindre ses objectifs commerciaux sur son site de déploiement principal. Ces événements peuvent être des

catastrophes naturelles, des défaillances techniques ou le résultat d'actions humaines, telles qu'une mauvaise configuration involontaire ou une attaque de logiciel malveillant.

reprise après sinistre (DR)

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

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

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

DR

Voir reprise après sinistre.

détection de dérive

Suivi des écarts par rapport à une configuration de référence. Par exemple, vous pouvez l'utiliser AWS CloudFormation pour détecter la dérive des ressources du système ou AWS Control Tower pour détecter les modifications de votre zone d'atterrissage susceptibles d'affecter le respect des exigences de gouvernance.

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

EDI

Voir échange de données informatisé.

informatique de périphérie

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

échange de données informatisé (EDI)

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

chiffrement

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

clé de chiffrement

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

endianisme

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

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

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

planification des ressources d'entreprise (ERP)

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

chiffrement d'enveloppe

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

environment

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

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

épopée

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

ERP

Voir Planification des ressources d'entreprise.

analyse exploratoire des données (EDA)

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

F

tableau des faits

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

échouer rapidement

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

limite d'isolation des défauts

Dans le AWS Cloud, une limite telle qu'une zone de disponibilité Région AWS, un plan de contrôle ou un plan de données qui limite l'effet d'une panne et contribue à améliorer la résilience des charges de travail. Pour plus d'informations, consultez la section Limites d'isolation des AWS pannes.

branche de fonctionnalités

Voir succursale.

fonctionnalités

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

importance des fonctionnalités

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

transformation de fonctionnalité

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

invitation en quelques coups

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

FGAC

Découvrez le contrôle d'accès détaillé.

contrôle d'accès détaillé (FGAC)

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

migration instantanée (flash-cut)

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

FM

Voir le modèle de fondation.

modèle de fondation (FM)

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

G

IA générative

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

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

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

Flux de travail Gitflow

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

image dorée

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

stratégie inédite

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

barrière de protection

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

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

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

haute disponibilité (HA)

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

modernisation des historiens

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

données de rétention

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

migration de base de données homogène

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

données chaudes

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

correctif

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

période de soins intensifs

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

I

IaC

Considérez l'infrastructure comme un code.

politique basée sur l’identité

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

application inactive

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

IIo T

Voir Internet industriel des objets.

infrastructure immuable

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

VPC entrant (d'entrée)

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

migration incrémentielle

Stratégie de basculement dans le cadre de laquelle vous migrez votre application par petites parties au lieu d'effectuer un basculement complet unique. Par exemple, il se peut que vous ne transfériez que quelques microservices ou utilisateurs vers le nouveau système dans un premier temps. Après avoir vérifié que tout fonctionne correctement, vous pouvez transférer

progressivement des microservices ou des utilisateurs supplémentaires jusqu'à ce que vous puissiez mettre hors service votre système hérité. Cette stratégie réduit les risques associés aux migrations de grande ampleur.

Industry 4.0

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

infrastructure

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

infrastructure en tant que code (IaC)

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

Internet industriel des objets (IIoT)

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

VPC d'inspection

Dans une architecture AWS multi-comptes, un VPC centralisé qui gère les inspections du trafic réseau VPCs entre (identique ou Régions AWS différent), Internet et les réseaux locaux. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

Internet des objets (IoT)

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

interprétabilité

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

IoT

Voir Internet des objets.

Bibliothèque d'informations informatiques (ITIL)

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

gestion des services informatiques (ITSM)

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

ITIL

Consultez la bibliothèque d'informations informatiques.

ITSM

Voir Gestion des services informatiques.

L

contrôle d'accès basé sur des étiquettes (LBAC)

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

zone de destination

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

grand modèle de langage (LLM)

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

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'accès basé sur des étiquettes.

principe de moindre privilège

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

lift and shift

Voir 7 Rs.

système de poids faible

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

LLM

Voir le grand modèle de langage.

environnements inférieurs

Voir environnement.

M

machine learning (ML)

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

branche principale

Voir succursale.

malware

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

services gérés

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

système d'exécution de la fabrication (MES)

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

MAP

Voir Migration Acceleration Program.

mécanisme

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

compte membre

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

MAILLES

Voir le système d'exécution de la fabrication.

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

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

microservice

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

architecture de microservices

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

Programme d'accélération des migrations (MAP)

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

migration à grande échelle

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

usine de migration

Équipes interfonctionnelles qui rationalisent la migration des charges de travail grâce à des approches automatisées et agiles. Les équipes de Migration Factory comprennent généralement des responsables des opérations, des analystes commerciaux et des propriétaires, des ingénieurs de migration, des développeurs et DevOps des professionnels travaillant dans le cadre de sprints.

Entre 20 et 50 % du portefeuille d'applications d'entreprise est constitué de modèles répétés qui peuvent être optimisés par une approche d'usine. Pour plus d'informations, veuillez consulter la rubrique discussion of migration factories et le guide Cloud Migration Factory dans cet ensemble de contenus.

métadonnées de migration

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

modèle de migration

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

Évaluation du portefeuille de migration (MPA)

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

Évaluation de la préparation à la migration (MRA)

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

stratégie de migration

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

ML

Voir apprentissage automatique.

modernisation

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

évaluation de la préparation à la modernisation

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

applications monolithiques (monolithes)

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

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

classification multi-classes

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

infrastructure mutable

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

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

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

OI

Voir Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

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

OPC-UA

Voir Open Process Communications - Architecture unifiée.

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

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

accord au niveau opérationnel (OLA)

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

examen de l'état de préparation opérationnelle (ORR)

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

technologie opérationnelle (OT)

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

intégration des opérations (OI)

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

journal de suivi d'organisation

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

gestion du changement organisationnel (OCM)

Cadre pour gérer les transformations métier majeures et perturbatrices du point de vue des personnes, de la culture et du leadership. L'OCM aide les organisations à se préparer et à effectuer la transition vers de nouveaux systèmes et de nouvelles politiques en accélérant

l'adoption des changements, en abordant les problèmes de transition et en favorisant des changements culturels et organisationnels. Dans la stratégie de AWS migration, ce cadre est appelé accélération du personnel, en raison de la rapidité du changement requise dans les projets d'adoption du cloud. Pour plus d'informations, veuillez consulter le guide OCM.

contrôle d'accès d'origine (OAC)

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

identité d'accès d'origine (OAI)

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

ORR

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

DE

Voir technologie opérationnelle.

VPC sortant (de sortie)

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

P

limite des autorisations

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

informations personnelles identifiables (PII)

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

PII

Voir les informations personnelles identifiables.

manuel stratégique

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

PLC

Voir contrôleur logique programmable.

PLM

Consultez la section Gestion du cycle de vie des produits.

politique

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

persistance polyglotte

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

évaluation du portefeuille

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

predicate

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

prédicat pushdown

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

contrôle préventif

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

principal

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

confidentialité dès la conception

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

zones hébergées privées

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

contrôle proactif

Contrôle de sécurité conçu pour empêcher le déploiement de ressources non conformes. Ces contrôles analysent les ressources avant qu'elles ne soient provisionnées. Si la ressource n'est

pas conforme au contrôle, elle n'est pas provisionnée. Pour plus d'informations, consultez le guide de référence sur les contrôles dans la AWS Control Tower documentation et consultez la section Contrôles proactifs dans Implémentation des contrôles de sécurité sur AWS.

gestion du cycle de vie des produits (PLM)

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

environnement de production

Voir environnement.

contrôleur logique programmable (PLC)

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

chaînage rapide

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

pseudonymisation

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

publish/subscribe (pub/sub)

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

Q

plan de requête

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

régression du plan de requêtes

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

R

Matrice RACI

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

CHIFFON

Voir Retrieval Augmented Generation.

rançongiciel

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

Matrice RASCI

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

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

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

réarchitecte

Voir 7 Rs.

objectif de point de récupération (RPO)

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

objectif de temps de récupération (RTO)

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

refactoriser

Voir 7 Rs.

Région

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

régression

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

réhéberger

Voir 7 Rs.

version

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

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

résilience

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

politique basée sur les ressources

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

matrice responsable, redevable, consulté et informé (RACI)

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

contrôle réactif

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

retain

Voir 7 Rs.

se retirer

Voir 7 Rs.

Génération augmentée de récupération (RAG)

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

rotation

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

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

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

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif relatif au temps de rétablissement.

runbook

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

S

SAML 2.0

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

SCADA

Voir Contrôle de supervision et acquisition de données.

SCP

Voir la politique de contrôle des services.

secret

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

sécurité dès la conception

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

contrôle de sécurité

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

renforcement de la sécurité

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

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

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

automatisation des réponses de sécurité

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

chiffrement côté serveur

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

Politique de contrôle des services (SCP)

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

point de terminaison du service

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

contrat de niveau de service (SLA)

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

indicateur de niveau de service (SLI)

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

objectif de niveau de service (SLO)

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

modèle de responsabilité partagée

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

SIEM

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

point de défaillance unique (SPOF)

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

SLA

Voir le contrat de niveau de service.

SLI

Voir l'indicateur de niveau de service.

SLO

Voir l'objectif de niveau de service.

split-and-seed modèle

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

SPOF

Voir point de défaillance unique.

schéma en étoile

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

modèle de figuier étrangleur

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

sous-réseau

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

contrôle de supervision et acquisition de données (SCADA)

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

chiffrement symétrique

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

tests synthétiques

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

invite du système

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

T

balises

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

variable cible

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

liste de tâches

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

environnement de test

Voir environnement.

entraînement

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

passerelle de transit

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

flux de travail basé sur jonction

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

accès sécurisé

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

réglage

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

équipe de deux pizzas

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

U

incertitude

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

tâches indifférenciées

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

environnements supérieurs

Voir environnement.

V

mise à vide

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

contrôle de version

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

Appairage de VPC

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

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

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

données chaudes

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

fonction de fenêtre

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

charge de travail

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

flux de travail

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

VER

Voir écrire une fois, lire plusieurs.

WQF

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

écrire une fois, lire plusieurs (WORM)

Modèle de stockage qui écrit les données une seule fois et empêche leur suppression ou leur modification. Les utilisateurs autorisés peuvent lire les données autant de fois que nécessaire,

mais ils ne peuvent pas les modifier. Cette infrastructure de stockage de données est considérée comme immuable.

Z

exploit Zero-Day

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

vulnérabilité « jour zéro »

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

invite Zero-Shot

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

application zombie

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

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