AWS Key Management Service meilleures pratiques

AWS Conseils prescriptifs

AWS Conseils prescriptifs: 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 Gestion des identités et des accès AWS (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 Gestion des identités et des accès AWS (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 sur la façon de 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 suivi 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. Gestion des identités et des accès AWS 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 instances Amazon EC2. 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 à un 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, AWS KMS vos politiques clés doivent autoriser le rôle lié au service à utiliser votre clé KMS pour certaines opérations d'API, par exemple pour `Decrypt` 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 instance Amazon EC2.
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 instance Amazon EC2. Pour obtenir des instructions, consultez Lancer une instance Amazon EC2.
5. Attachez le volume que vous avez créé à l'instance Amazon EC2. Pour obtenir des instructions, consultez Attacher un volume Amazon EBS à une instance Amazon EC2.
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 documentation Amazon EC2.

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 Gestion des identités et des accès AWS (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.

Meilleures 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 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 Surveillance des clés KMS avec les CloudWatch alarmes Amazon 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 CSPM. Security Hub CSPM 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 Gestion des identités et des accès AWS (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 CSPM. 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 Console de gestion AWS 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

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.