Les 10 meilleures pratiques de sécurité pour sécuriser les sauvegardes dans AWS

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Les 10 meilleures pratiques de sécurité pour sécuriser les sauvegardes dans AWS

Table of Contents

Les 10 meilleures pratiques de sécurité pour sécuriser les sauvegardes dans AWS

Ibukun (IB) Oyewumi, Amazon Web Services (AWS)

Mai 2022 (historique du document)

La sécurité est une responsabilité partagée entre Amazon Web Services (AWS) et ses clients. Les clients ont demandé des moyens de sécuriser leurs sauvegardes dans AWS. Les pratiques de sécurité évoluant constamment pour atténuer les nouveaux risques, il est important que vous réalisiez régulièrement des évaluations des risques afin de déterminer l'applicabilité des contrôles de sécurité et que vous implémentiez plusieurs niveaux de contrôles pour atténuer les risques pour vos données.

Ce document vous guidera à travers une liste organisée des 10 meilleures pratiques de sécurité pour sécuriser vos données de sauvegarde et vos opérations dans AWS. Bien que ce guide se concentre sur les données et les opérations de sauvegarde à l'aide du service AWS Backup, ces bonnes pratiques de sécurité recommandées peuvent être utilisées avec d'autres solutions de sauvegarde, telles que les outils de sauvegarde d'AWS Marketplace.

Bonnes pratiques

Lorsque vous sécurisez des sauvegardes dans AWS, nous vous recommandons d'utiliser l'approche suivante :

Rubriques

Étape 1. Implémenter une stratégie de sauvegarde

Une stratégie de sauvegarde complète est un élément essentiel du plan de protection des données d'une organisation afin de résister à un événement de sécurité, de s'en remettre et d'en réduire l'impact éventuel. Créez une stratégie de sauvegarde complète qui définit les données à sauvegarder, à quelle fréquence et comment les tâches de sauvegarde et de restauration seront surveillées.

Lorsque vous élaborez une stratégie complète de sauvegarde et de restauration des données, identifiez d'abord les interruptions susceptibles de se produire, ainsi que leur impact potentiel sur l'activité.

Votre objectif est de générer une stratégie de reprise qui rétablit votre charge de travail ou évite les temps d'arrêt dans les limites acceptables des objectifs de reprise, des objectifs de délai de reprise (RTO) et des objectifs de point de reprise (RPO). Le RTO est le délai acceptable entre l'interruption du service et son rétablissement. Le RPO est le délai acceptable depuis le dernier point

de récupération des données. Envisagez une stratégie de sauvegarde détaillée incluant tous les éléments suivants :

- Cadence de sauvegarde continue
- Point-in-Time Rétablissement (PITR)
- Récupération au niveau du fichier
- Récupération au niveau des données d'application
- Récupération au niveau du volume
- Récupération au niveau de l'instance

Rançongiciel

Une stratégie de sauvegarde bien conçue doit inclure des actions permettant de protéger et de récupérer vos ressources après une attaque par rançongiciel, avec des exigences de récupération détaillées pour vos applications et leurs dépendances en matière de données. Par exemple, lorsque vous établissez des contrôles préventifs et de détection pour atténuer le risque de ransomware, veillez également à définir le niveau de granularité approprié pour les modèles de copie et de restauration entre comptes Région AWS ou entre comptes, afin de garantir que les administrateurs ne restaurent pas les données de sauvegarde corrompues après l'événement de sécurité.

Exigences de conservation

Dans certains secteurs, lors de l'élaboration d'une stratégie de sauvegarde, vous devez également tenir compte des réglementations relatives aux exigences de conservation des données. Assurez-vous que votre stratégie de sauvegarde est conçue avec des exigences de conservation suffisantes pour répondre à vos besoins réglementaires pour chaque niveau de classification des données et chaque type de ressource.

Conformité d’

Consultez vos équipes chargées de la conformité en matière de sécurité pour déterminer si vos ressources et opérations de sauvegarde doivent être incluses ou segmentées dans le cadre de vos programmes de conformité. L'inclusion de la sauvegarde et de la restauration comme éléments essentiels de votre programme de sécurité vous aidera à comprendre où se situent les données dans votre environnement et à définir correctement la portée de la conformité.

Pour connaître les meilleures pratiques architecturales relatives à la conception et à l'exploitation de charges de travail fiables, sécurisées, efficaces et rentables dans le cloud, voir Backup and recovery approaches using AWS and Reliability Pillar — AWS Well-Architected Framework.

Étape 2. Intégrer la sauvegarde dans la DR et le BCP

La reprise après sinistre (DR) est le processus de préparation, de réponse et de reprise après un sinistre. Élément important de votre stratégie de résilience, le plan de reprise après sinistre concerne le mode de réponse de votre charge de travail en cas de sinistre. Un sinistre peut être une défaillance technique, une action humaine ou un événement naturel. Le plan de continuité des activités (BCP) décrit la manière dont une organisation entend poursuivre ses activités commerciales normales en cas d'interruption imprévue.

Votre plan de reprise après sinistre doit être un sous-ensemble du BCP de votre organisation. Le BCP doit également inclure des AWS Backup procédures. Par exemple, un événement de sécurité affectant les données de production peut vous obliger à invoquer un plan de reprise après sinistre qui utilise AWS Backup le basculement pour sauvegarder les données d'un autre Région AWS. Assurez-vous que vos employés connaissent les procédures de votre organisation et AWS Backup qu'ils se sont entraînés à les utiliser, afin qu'en cas de sinistre, votre organisation puisse poursuivre ses activités normales avec peu ou pas d'interruption de service. Plus d'informations sur l'utilisation AWS Backup sont fournies dans d'autres sections de ce guide.

Étape 3. Automatiser vos opérations de sauvegarde

Les plans de sauvegarde et les affectations de ressources de votre organisation doivent être configurés pour refléter les politiques de protection des données de votre entreprise. En automatisant et en déployant des stratégies de sauvegarde ou des plans de sauvegarde à l'échelle de l'organisation, vous pouvez normaliser et mettre à l'échelle votre stratégie de sauvegarde. Vous pouvez utiliser AWS Organizations pour automatiser de manière centralisée les politiques de sauvegarde afin d'implémenter, de configurer, de gérer et de régir les activités de sauvegarde dans les ressources AWS Backup prises en charge en planifiant des opérations de sauvegarde.

Pour améliorer la productivité et régir les opérations d'infrastructure dans des environnements à comptes multiples, envisagez d'implémenter l'infrastructure en tant que code (IaC) et une architecture axée sur les événements pour en faire des éléments essentiels de votre transformation numérique et de votre stratégie de sauvegarde. L'automatisation des sauvegardes offre les avantages suivants :

- Réduction de la surcharge manuelle liée à la configuration fastidieuse de vos sauvegardes

- Minimisation du risque d'erreurs
- Visibilité sur la détection de la dérive
- Améliore le respect des politiques de sauvegarde pour plusieurs AWS charges de travail ou comptes

L'implémentation de politiques de sauvegarde en tant que code peut vous aider à respecter les réglementations en matière de protection des données en procédant comme suit :

- Configuration de différentes exigences pour vos types de ressource
- Mise à l'échelle de la stratégie de protection des données de votre entreprise
- Implémentation de règles du cycle de vie pour spécifier le délai avant qu'un point de récupération ne passe au stockage à froid ou soit supprimé, ce qui peut vous aider à optimiser vos coûts

Lorsque vous automatisez vos opérations de sauvegarde, vous pouvez adapter les options d'affectation des ressources en utilisant des AWS balises et des ressources IDs pour identifier automatiquement les AWS ressources qui stockent les données pour vos applications critiques et protègent vos données à l'aide de sauvegardes immuables. Cela peut vous aider à prioriser les contrôles de sécurité, tels que les autorisations d'accès et les plans ou politiques de sauvegarde.

Étape 4 : Implémenter des mécanismes de contrôle d'accès

Lorsque vous pensez à la sécurité dans le cloud, votre stratégie de base doit commencer par une base d'identité solide afin de garantir que les utilisateurs disposent des autorisations appropriées pour accéder aux données. Une authentification et une autorisation appropriées peuvent atténuer le risque d'événements de sécurité. Le modèle de responsabilité partagée oblige AWS les clients à mettre en œuvre des politiques de contrôle d'accès. Pour créer et gérer des politiques d'accès à grande échelle, vous pouvez utiliser Gestion des identités et des accès AWS (IAM).

Pour configurer vos droits et autorisations d'accès, appliquez le principe du moindre privilège en vous assurant que chaque utilisateur ou système accédant à vos données de sauvegarde ou à votre coffre-fort reçoive uniquement les permissions nécessaires pour accomplir ses tâches. AWS Backup À utiliser pour définir des politiques d'accès aux coffres-forts de sauvegarde afin de protéger vos charges de travail dans le cloud.

Par exemple, en implémentant des politiques de contrôle d'accès, vous pouvez autoriser les utilisateurs à créer des plans de sauvegarde et des sauvegardes à la demande tout en limitant leur

capacité à supprimer des points de restauration. À l'aide des politiques d'accès au coffre-fort, vous pouvez partager un coffre-fort de sauvegarde de destination avec un rôle source Compte AWS ou IAM, selon les besoins de votre entreprise. Vous pouvez également utiliser des politiques d'accès pour partager un coffre-fort de sauvegarde avec un ou plusieurs comptes, ou avec l'ensemble de votre organisation dans AWS Organizations. Pour plus d'informations, consultez la documentation AWS Backup.

Au fur et à mesure que vous augmentez vos charges de travail ou que vous migrez vers AWS, vous devrez peut-être gérer de manière centralisée les autorisations relatives à vos coffres-forts de sauvegarde et à vos opérations. Utilisez les politiques de contrôle des services (SCPs) pour mettre en œuvre un contrôle centralisé des autorisations maximales disponibles pour tous les comptes de votre organisation. SCPs offrent une défense approfondie et garantissent que vos utilisateurs respectent les directives de contrôle d'accès définies. Pour plus d'informations, veuillez consulter Managing access to backups using service control policies with AWS Backup.

Pour atténuer les risques de sécurité tels que l'accès involontaire à vos ressources et données de sauvegarde, utilisez IAM Access Analyzer pour identifier tout rôle AWS Backup IAM partagé avec les entités suivantes :

- Une entité externe telle qu'un Compte AWS
- Un utilisateur root
- Un utilisateur ou un rôle IAM
- Un utilisateur fédéré
- Un Service AWS
- Un utilisateur anonyme
- Toute autre entité pouvant être utilisée pour créer un filtre

Étape 5. Chiffrer les données de sauvegarde et le coffre-fort

Les organisations doivent améliorer de plus en plus leur stratégie de sécurité des données, et elles peuvent être amenées à respecter les réglementations en matière de protection des données lorsqu'elles sont mises à l'échelle dans le cloud. L'implémentation correcte des méthodes de chiffrement peut fournir un niveau de protection supplémentaire par rapport aux mécanismes de contrôle d'accès de base. Ce niveau supplémentaire fournit une solution d'atténuation en cas d'échec de vos principales politiques de contrôle d'accès.

Par exemple, si vous configurez des politiques de contrôle d'accès trop permissives sur vos données AWS Backup , votre système ou votre processus de gestion des clés peuvent atténuer l'impact maximal d'un événement de sécurité. En effet, il existe des mécanismes d'autorisation distincts pour accéder à vos données et à votre clé de chiffrement, ce qui signifie que les données de sauvegarde ne sont visibles que sous forme de texte chiffré.

Pour tirer le meilleur parti du AWS Cloud chiffrement, chiffrez les données en transit et au repos. Pour protéger les données en transit, AWS utilise des appels d'API publiés pour accéder AWS Backup via le réseau à l'aide du protocole TLS afin d'assurer le chiffrement entre vous, votre application et le AWS Backup service. Pour protéger les données au repos, vous pouvez utiliser AWS cloud-native AWS Key Management Service(AWS KMS) ou AWS CloudHSM. En tant que modèle de sécurité matérielle (HSM) basé sur le cloud, AWS CloudHSM utilise la norme Advanced Encryption Standard (AES) avec des clés de 256 bits (AES-256), un puissant algorithme adopté par le secteur pour chiffrer des données. Évaluez la gouvernance de vos données et les exigences réglementaires, puis sélectionnez le service de chiffrement approprié pour chiffrer vos données cloud et vos coffres-forts de sauvegarde.

La configuration du chiffrement varie en fonction du type de ressource et des opérations de sauvegarde selon les comptes ou les régions. Certains types de ressource prennent en charge la possibilité de chiffrer vos sauvegardes à l'aide d'une clé de chiffrement différente de celle utilisée pour chiffrer la ressource source. Étant donné que vous êtes chargé de gérer les contrôles d'accès afin de déterminer qui peut accéder à vos AWS Backup données ou aux clés de chiffrement de votre coffre-fort et dans quelles conditions, utilisez le langage de politique proposé par AWS KMS pour définir les contrôles d'accès aux clés. Vous pouvez également utiliser AWS Backup Audit Manager pour vérifier que votre sauvegarde est correctement chiffrée. Pour plus d'informations, veuillez consulter Encryption for backups in AWS Backup.

Vous pouvez utiliser des clés multi-régions AWS KMS pour répliquer les clés d'une région à l'autre. Les clés multi-régions visent à simplifier la gestion du chiffrement lorsque vos données chiffrées doivent être copiées dans d'autres régions pour une reprise après sinistre. Évaluez la nécessité d'implémenter des AWS KMS clés multirégionales dans le cadre de votre stratégie de sauvegarde globale.

Étape 6. Protéger les sauvegardes à l'aide d'un stockage immuable

Les organisations peuvent utiliser le stockage immuable pour écrire des données à l'état WORM (Write Once Read Many). À l'état WORM, les données peuvent être écrites une seule fois, puis lues

et utilisées aussi souvent que nécessaire une fois qu'elles ont été validées ou écrites sur le support de stockage. Le stockage immuable permet de garantir le maintien de l'intégrité des données. Il offre également une protection contre les éléments suivants :

- Suppressions
- Écrasements
- Accès involontaire et non autorisé
- Compromission par un rançongiciel

Le stockage immuable propose un mécanisme efficace pour faire face aux événements de sécurité potentiels susceptibles d'avoir un impact réel sur vos opérations métier.

Vous pouvez utiliser le stockage immuable pour améliorer la gouvernance lorsqu'il est associé à des restrictions SCP fortes. Vous pouvez également utiliser le stockage immuable en mode WORM de conformité lorsque la lettre de la loi (telle qu'une mise en suspens juridique) exige l'accès à des données immuables.

Pour garantir la disponibilité et l'intégrité des données, vous pouvez utiliser AWS Backup Vault Lock et ainsi protéger vos sauvegardes. Lorsque vous utilisez AWS Backup Vault Lock, les entités non autorisées ne peuvent pas effacer, modifier ou corrompre les données de vos clients ou de votre entreprise pendant la période de conservation requise. AWS Backup Vault Lock vous aide à respecter les politiques de protection des données de votre entreprise en empêchant ce qui suit :

- Suppressions effectuées par des utilisateurs privilégiés (y compris l'utilisateur Compte AWS root)
- Modifications apportées à vos paramètres du cycle de vie des sauvegardes
- Mises à jour modifiant la période de conservation que vous avez définie

AWS Backup Vault Lock garantit l'immuabilité et ajoute une couche de défense supplémentaire qui protège les sauvegardes (points de restauration) dans vos coffres-forts de sauvegarde. Cela est particulièrement utile dans les secteurs hautement réglementés qui ont des besoins d'intégrité stricts pour les sauvegardes et les archives. AWS Backup Vault Lock s'assure que vos données sont préservées, ainsi qu'une sauvegarde à récupérer en cas d'actions involontaires ou malveillantes.

⚠ Important

- AWS Backup La conformité de Vault Lock à la règle 17a-4 (f) de la Securities and Exchange Commission (SEC) et à la réglementation 17 C.F.R. 1.31 (b) à (c) de la Commodity Futures Trading Commission (CFTC) n'a pas encore été évaluée.
- AWS Backup Vault Lock prend effet immédiatement. Vous bénéficiez alors d'une période de réflexion minimale de trois jours (72 heures) pour supprimer ou mettre à jour sa configuration avant de verrouiller définitivement votre coffre-fort. Vous pouvez éventuellement prolonger la durée de cette période de réflexion. Profitez de cette période de réflexion pour tester AWS Backup Vault Lock par rapport à vos charges de travail et à vos cas d'utilisation. Une fois votre période de réflexion expirée, vous ne AWS Support pouvez ni supprimer ni modifier AWS Backup Vault Lock ou le contenu de votre coffre-fort verrouillé. Pour plus d'informations, veuillez consulter la documentation sur AWS Backup Vault Lock.

Étape 7. Implémenter la surveillance des sauvegardes et les alertes

Les tâches de sauvegarde peuvent échouer. L'échec d'une tâche, telle qu'une tâche de sauvegarde, de restauration ou de copie, peut avoir un impact sur les étapes ultérieures d'un processus. Lorsque la tâche de sauvegarde initiale échoue, il est très probable que les autres tâches suivantes échouent également. Dans un tel cas, vous pouvez mieux comprendre le cours des événements grâce à la surveillance et à la notification. La surveillance et les alertes peuvent permettre à l'organisation de prendre conscience de vos tâches de sauvegarde, ce qui vous aide à faire face aux défaillances de sauvegarde.

L'activation et la configuration des notifications pour surveiller les tâches AWS Backup offrent les avantages suivants :

- Vous sensibiliser à vos activités de sauvegarde
- Permet de garantir que vous respectez les accords de niveau de service essentiels () SLAs
- Améliore votre business-as-usual surveillance
- Respecter vos obligations de conformité

Vous pouvez mettre en œuvre une surveillance des sauvegardes pour vos charges de travail en les intégrant à d'autres systèmes Services AWS et AWS Backup à des systèmes de billetterie afin d'effectuer des enquêtes automatisées et des flux d'escalade. Par exemple, vous pouvez effectuer les opérations suivantes :

- Utilisez Amazon CloudWatch pour suivre les métriques, créer des alarmes et consulter des tableaux de bord.
- Utilisez Amazon EventBridge pour surveiller AWS Backup les processus et les événements.
- Utilisez AWS CloudTrail pour surveiller des appels d'API AWS Backup avec des informations détaillées sur l'heure, l'adresse IP source, les utilisateurs et les comptes effectuant ces appels.
- Utilisez Amazon Simple Notification Service (Amazon SNS) pour vous abonner AWS Backup à des sujets connexes tels que les événements de sauvegarde, de restauration et de copie.

Vous pouvez utiliser AWS Backup Audit Manager pour générer automatiquement des preuves de vos rapports d'audit de sauvegarde quotidiens pour chaque compte et région. Vous pouvez également étendre la surveillance des sauvegardes à plusieurs comptes en utilisant un ensemble de modèles d'automatisation et de tableaux de bord (connus sous le nom de solution Backup Observer) pour obtenir des rapports quotidiens agrégés entre comptes et AWS Backup multirégions.

Étape 8. Configuration des sauvegardes d'audit

Pour vous assurer que le programme de sauvegarde fonctionne comme il se doit et pour identifier et corriger toute anomalie liée aux processus de sauvegarde, vérifiez la conformité des AWS Backup politiques par rapport aux contrôles définis, tels que la fréquence de sauvegarde définie. Pour identifier et examiner les opérations ou les ressources de sauvegarde qui ne sont pas conformes à vos exigences métier, suivez en permanence et automatiquement votre activité de sauvegarde et générez des rapports automatiques.

AWS Backup Audit Manager fournit des contrôles de conformité intégrés et personnalisables qui s'alignent sur les exigences réglementaires et de conformité de votre entreprise. Vous pouvez utiliser des contrôles prédéfinis et personnalisables sous forme de cadres d'audit pour évaluer vos pratiques AWS Backup . Ces contrôles sont les suivants :

- Ressources de sauvegarde protégées par des plans de sauvegarde
- Fréquence minimale du plan de sauvegarde et conservation minimale
- Point de restauration de sauvegarde chiffré

- Suppression manuelle du point de restauration de sauvegarde
- Conservation minimale du point de restauration de sauvegarde
- Copie entre régions
- Copie entre comptes
- Backup Vault Lock

Pour automatiser l'infrastructure en tant que code (IaC), vous pouvez utiliser AWS Backup Audit Manager avec AWS CloudFormation.

AWS Security Hub CSPMvous fournit une vue complète de votre état de sécurité dans AWS. Il vous permet également de vérifier que votre environnement est conforme aux bonnes pratiques en matière de sécurité et aux normes du secteur, telles que les contrôles Pratiques exemplaires en matière de sécurité de base AWS. Si vous utilisez Security Hub CSPM dans votre environnement cloud, nous vous recommandons d'activer la norme AWS Foundational Security Best Practices, car elle inclut des contrôles de détection qui peuvent aider à sécuriser les sauvegardes dans. AWS La plupart des contrôles de détection AWS Backup d'Audit Manager et de Security Hub CSPM sont également disponibles sous forme de règles AWS Config gérées.

Étape 9. Tester les capacités de récupération des données

Votre stratégie de sauvegarde doit inclure le test de vos sauvegardes. Une stratégie de sauvegarde n'est pas efficace si les données sauvegardées ne peuvent pas être restaurées. Testez régulièrement votre capacité à trouver certains points de récupération et à les restaurer.

Bien que les balises soient AWS Backup automatiquement copiées depuis les ressources qu'elle protège vers les points de restauration, les balises ne sont pas copiées par défaut des points de restauration vers les ressources restaurées correspondantes. Pour étendre votre gestion des stocks et localiser les points de récupération, pensez à utiliser AWS Backup des événements pour lancer un processus de réplication de balises sur les ressources créées par les tâches de AWS Backup restauration.

Vous pouvez démarrer votre flux de travail de récupération de données en établissant des modèles de récupération de données, puis en les testant régulièrement. Pour renforcer la confiance dans votre capacité à restaurer les données de sauvegarde, créez un processus de base reproductible pour effectuer des tests de récupération continue des données. Par exemple, vous pouvez créer un modèle pour tester une opération de restauration entre comptes et entre régions à partir d'un coffre-

fort de sauvegarde DR central chiffré avec une clé AWS KMS gérée par le client vers un coffre-fort de sauvegarde d'un compte source chiffré par une autre clé AWS KMS gérée par le client.

Si vous ne testez pas fréquemment de telles opérations de restauration, vous constaterez peut-être que vos hypothèses concernant le AWS KMS chiffrement des opérations entre comptes et entre régions sont incorrectes. Souvent, le seul modèle de récupération des sauvegardes qui fonctionne réellement est le chemin que vous testez fréquemment. Grâce à des tests de routine des types de ressource de sauvegarde pris en charge, vous pouvez détecter les alertes précoces susceptibles de provoquer de futures perturbations et la perte de données critiques. Si possible, maintenez un nombre limité, mais praticable, de chemins et de modèles de restauration afin d'éviter le gaspillage d'espace de stockage, d'optimiser les coûts et de gagner du temps. Il est plus facile de résoudre le problème en cas d'échec d'un test de restauration que de perdre des données importantes ou critiques.

Étape 10. Intégrer la sauvegarde dans votre plan de réponse aux incidents

Les simulations de réponse aux incidents de sécurité (SIRS) sont des événements internes qui offrent une opportunité structurée de mettre en pratique votre plan et vos procédures de réponse aux incidents dans le cadre d'un scénario réaliste. Il est utile de tester vos données et opérations de sauvegarde dans le cadre d'activités SIRS créatives afin de vous tester face aux imprévus. Cela vous aide à valider votre état de préparation organisationnelle et à vous sentir à l'aise face aux événements rares et inattendus. Vos simulations doivent être réalistes et impliquer des équipes organisationnelles interfonctionnelles qui sont tenues de répondre aux événements.

Commencez par des exercices de simulation de base et dirigez-vous vers un événement complet et complexe. Par exemple, vous pouvez générer un modèle réaliste composé d'un cloud privé virtuel (VPC) et de ressources associées qui simulent une surexposition involontaire d'informations ou une violation potentielle de données provoquée par des modifications apportées aux politiques et aux listes de contrôle d'accès. Pour évaluer le bon fonctionnement de votre plan de réponse aux incidents, documentez les enseignements tirés et identifiez les améliorations à apporter aux futures procédures de réponse.

Vous pouvez l'utiliser AWS Backup pour configurer des sauvegardes automatisées au niveau de l'instance sous la forme d'Amazon Machine Images (AMIs) et des sauvegardes au niveau du volume sous forme de snapshots sur plusieurs. Comptes AWS Cela peut aider votre équipe de réponse aux incidents à améliorer ses processus d'investigation, tels que la collecte de disques légale

automatisée, en fournissant un point de restauration susceptible de réduire la portée et l'impact d'événements de sécurité potentiels tels que les rançongiciels.

Étapes suivantes

Ce guide décrit les 10 meilleures pratiques et contrôles de sécurité pour protéger vos données de sauvegarde dans AWS. Nous vous recommandons d'utiliser ces bonnes pratiques pour concevoir et implémenter une stratégie et une architecture de sauvegarde et de restauration, avec plusieurs niveaux de contrôles, qui s'adaptent et répondent aux besoins de votre entreprise. Pour plus d'informations AWS Backup, consultez la AWS Backup documentation.

Si vous avez des questions concernant ce guide, créez un nouveau fil de discussion sur le forum AWS Backup ou contactez AWS Support.

Ressources

AWS Conseils prescriptifs

- Backup and recovery approaches on AWS (guide)

AWS documentation

- AWS Backup
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon EventBridge
- IAM
- AWS KMS
- AWS Organizations
- AWS Security Hub CSPM
- Amazon SNS

Billets de blogs

- Automatisez la sauvegarde centralisée à grande échelle Services AWS en utilisant AWS Backup
- Architecture de reprise après sinistre (DR) AWS, partie I : stratégies de reprise dans le cloud
- L'importance du chiffrement et comment il AWS peut y contribuer
- Améliorez le niveau de sécurité de vos sauvegardes avec AWS Backup Vault Lock
- Surveillez, évaluez et démontrez la conformité des sauvegardes avec AWS Backup Audit Manager
- Créez et partagez des sauvegardes chiffrées entre comptes et régions à l'aide de AWS Backup
- Simplifiez l'audit de vos politiques de protection des données avec AWS Backup Audit Manager

- Gestion de l'accès aux sauvegardes à l'aide de politiques de contrôle des services avec AWS Backup
- Obtenez des rapports quotidiens agrégés sur plusieurs comptes et multirégions AWS Backup

GitHub référentiels

Les référentiels de code suivants vous fournissent une solution de gestion et de déploiement pour mettre en œuvre la sauvegarde et la restauration au AWS Backup sein de votre AWS Organizations organisation, sur plusieurs comptes et Régions AWS.

- Mettre en œuvre en AWS Backup utilisant AWS
- Implémentation AWS Backup à l'aide de pipelines CI/CD

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	—	13 mai 2022

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.