Guide de l’utilisateur

AWS Audit Manager

AWS Audit Manager: Guide de l’utilisateur

Table of Contents

Qu'est-ce que c'est AWS Audit Manager ?

Bienvenue dans le guide de AWS Audit Manager l'utilisateur.

AWS Audit Manager vous aide à auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur. Audit Manager automatise la collecte d'éléments probants pour faciliter l'évaluation de l'efficacité de vos politiques, procédures et activités (également appelées contrôles). Lorsqu'il est temps d'effectuer un audit, Audit Manager vous aide à gérer les examens de vos contrôles par les parties prenantes. Cela signifie que vous pouvez créer des rapports prêts pour l'audit en fournissant moins d'efforts manuels.

Audit Manager fournit des frameworks prédéfinis qui structurent et automatisent les évaluations pour une norme ou une réglementation de conformité donnée. Les frameworks comprennent un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en fonction des exigences de la norme ou de la réglementation de conformité spécifiée. Vous pouvez également personnaliser les frameworks et les contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

Vous pouvez créer une évaluation à partir de n'importe quel framework. Lorsque vous créez une évaluation, Audit Manager exécute automatiquement des évaluations des ressources. Ces évaluations collectent des données pour Comptes AWS ce que vous définissez comme relevant du périmètre de votre audit. Les données collectées sont transformées automatiquement en éléments probants faciles à vérifier. Elles sont ensuite associées aux contrôles appropriés pour vous aider à démontrer la conformité en matière de sécurité, de gestion du changement, de continuité des activités et de licences logicielles. Ce processus de collecte d'éléments probants est continu et commence lorsque vous créez votre évaluation. Une fois que vous avez terminé un audit et que vous n'avez plus besoin d'Audit Manager pour recueillir des éléments probants, vous pouvez en arrêter la collecte. Pour ce faire, définissez le statut de votre évaluation sur inactive.

Fonctionnalités d'Audit Manager

Avec AWS Audit Manager, vous pouvez effectuer les tâches suivantes :

- Démarrez rapidement : créez votre première évaluation en choisissant parmi une galerie de frameworks prédéfinis qui prennent en charge un large éventail de normes et réglementations de conformité. Lancez ensuite la collecte automatique de preuves pour auditer votre Service AWS utilisation.

- Chargez et gérez les éléments probants provenant d'environnements hybrides ou multicloud : outre les éléments probants collectés par Audit Manager dans votre environnement AWS , vous pouvez également charger et gérer de manière centralisée les éléments probants issus de votre environnement sur site ou multicloud.
- Prise en charge des normes et réglementations de conformité communes : choisissez l'un des frameworks AWS Audit Manager standard. Ces frameworks fournissent des mappages de contrôle prédéfinis pour les normes et réglementations de conformité communes. Il s'agit notamment du CIS Foundation Benchmark, de la norme PCI DSS, du RGPD, de l'HIPAA, du SOC2, de la GxP et des meilleures pratiques opérationnelles. AWS
- Surveillez vos évaluations actives : utilisez le tableau de bord d'Audit Manager pour consulter les données analytiques relatives à vos évaluations actives et identifier rapidement les éléments probants non conformes qui doivent être corrigées.
- Recherche de preuves : utilisez Outil de recherche d'éléments probants cette fonctionnalité pour trouver rapidement des preuves pertinentes pour votre requête de recherche. Vous pouvez générer un rapport d'évaluation à partir de vos résultats de recherche ou les exporter au format CSV.
- Création de contrôles personnalisés : créez votre propre contrôle à partir de zéro ou créez une copie modifiable d'un contrôle standard ou personnalisé existant. Vous pouvez également utiliser la fonctionnalité de contrôles personnalisés pour créer des questions d'évaluation des risques et enregistrer les réponses à ces questions sous forme d'éléments probants manuels.
- Mappez les contrôles de votre entreprise à des groupes prédéfinis de sources de AWS données : choisissez les contrôles courants qui représentent vos objectifs et utilisez-les pour créer des contrôles personnalisés qui collectent des preuves pour votre portefeuille de besoins en matière de conformité.
- Création de cadres personnalisés — Créez vos propres cadres avec des contrôles standard ou personnalisés en fonction de vos exigences spécifiques en matière d'audits internes.
- Partagez des frameworks personnalisés : partagez vos frameworks Audit Manager personnalisés avec un autre Compte AWS, ou dupliquez-les dans un autre Région AWS sous votre propre compte.
- Prise en charge de la collaboration entre équipes : déléguez les ensembles de contrôle à des experts en la matière qui peuvent examiner les éléments probants connexes, ajouter des commentaires et mettre à jour le statut de chaque contrôle.
- Créez des rapports pour les auditeurs : générez des rapports d'évaluation qui résument les éléments probants pertinents collectés pour votre audit et renvoient à des dossiers contenant les éléments probants détaillés.

- Garantissez l'intégrité des éléments probants : stockez les éléments probants dans un endroit sûr, où ils ne seront pas modifiés.

> **Note**
>
> AWS Audit Manager aide à recueillir des preuves pertinentes pour vérifier la conformité aux normes et réglementations de conformité spécifiques. Cependant, il n'évalue pas votre conformité lui-même. Les preuves collectées par ce biais peuvent AWS Audit Manager donc ne pas inclure toutes les informations relatives à votre AWS utilisation nécessaires aux audits. AWS Audit Manager ne remplace pas un conseiller juridique ou un expert en conformité.

Tarification d'Audit Manager

Pour plus d'informations sur la tarification, consultez Tarification d'AWS Audit Manager.

Vous utilisez pour la première fois Audit Manager ?

Si vous utilisez Audit Manager pour la première fois, nous vous recommandons de commencer par consulter les pages suivantes :

1. Comprendre AWS Audit Manager les concepts et la terminologie— Découvrez les concepts et termes clés utilisés dans Audit Manager, tels que les évaluations, les cadres et les contrôles.
2. Comprendre le mode de AWS Audit Manager collecte des preuves— Découvrez comment Audit Manager collecte des preuves pour une évaluation des ressources.
3. Configuration AWS Audit Manager avec les paramètres recommandés— Découvrez les exigences de configuration pour Audit Manager.
4. Commencer avec AWS Audit Manager— Suivez un tutoriel pour créer votre première évaluation Audit Manager.
5. AWS Audit Manager Référence d'API — Familiarisez-vous avec les actions et les types de données de l'API Audit Manager.

Plus de ressources concernant Audit Manager

Consultez les ressources suivantes pour en savoir plus sur Audit Manager.

- Collectez des preuves et gérez les données d'audit à l'aide de AWS Audit Manager
- Modèle d'intégration à trois lignes (partie 2) : transformez les packs de AWS Config conformité en AWS Audit Manager évaluations, extrait du blog sur la AWS gestion et la gouvernance

Comprendre AWS Audit Manager les concepts et la terminologie

Pour vous aider à démarrer, cette rubrique explique certains des termes et concepts clés de AWS Audit Manager.

A

| B | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Évaluation

Vous pouvez utiliser une évaluation d'Audit Manager pour recueillir automatiquement les éléments probants pertinents pour un audit.

Une évaluation est basée sur un framework, qui est un regroupement de contrôles liés à votre audit. Vous pouvez créer une évaluation à partir d'un framework standard ou personnalisé. Les frameworks standard contiennent des ensembles de contrôle prédéfinis qui prennent en charge une norme ou une réglementation de conformité spécifique. En revanche, les frameworks personnalisés contiennent des contrôles que vous pouvez personnaliser et regrouper en fonction de vos exigences d'audit spécifiques. En utilisant un cadre comme point de départ, vous pouvez créer une évaluation qui précise Comptes AWS ce que vous souhaitez inclure dans le périmètre de votre audit.

Lorsque vous créez une évaluation, Audit Manager commence automatiquement à évaluer vos ressources en Comptes AWS fonction des contrôles définis dans le framework. Ensuite, il recueille les éléments probants pertinents et les convertit dans un format convivial pour les auditeurs. Ensuite, il joint les éléments probants aux contrôles de votre évaluation. Au moment d'effectuer un audit, vous (ou un délégué de votre choix) pouvez examiner les éléments probants recueillis, puis les ajouter à un rapport d'évaluation. Ce rapport d'évaluation vous aide à démontrer que vos contrôles fonctionnent comme prévu.

La collecte d'éléments probants est un processus continu et commence lorsque vous créez votre évaluation. Vous pouvez arrêter la collecte d'éléments probants en faisant passer le statut de l'évaluation sur inactive. Vous pouvez également l'arrêter au niveau du contrôle. Pour ce faire, vous pouvez faire passer le statut d'un contrôle spécifique de votre évaluation sur inactif.

Pour obtenir des instructions sur la façon de créer et de gérer des évaluations, veuillez consulter Gestion des évaluations dans AWS Audit Manager.

Rapport d'évaluation

Un rapport d'évaluation est un document finalisé généré à partir d'une évaluation d'Audit Manager. Ces rapports résument les éléments probants pertinents recueillis pour votre audit. Ils renvoient aux dossiers d'éléments probants appropriés. Les dossiers sont nommés et organisés conformément aux contrôles spécifiés dans votre évaluation. Pour chaque évaluation, vous pouvez passer en revue les éléments probants recueillis par Audit Manager et décider lesquels vous souhaitez inclure dans le rapport d'évaluation.

Pour en savoir plus sur les rapports d'évaluation, veuillez consulter Rapports d'évaluation. Pour savoir comment générer un rapport d'évaluation, veuillez consulter Préparation d'un rapport d'évaluation dans AWS Audit Manager.

Destination du rapport d'évaluation

Une destination de rapport d'évaluation est le compartiment S3 par défaut dans lequel Audit Manager enregistre vos rapports d'évaluation. Pour en savoir plus, veuillez consulter la section Configuration de la destination par défaut de votre rapport d'évaluation.

Audit

Un audit est un examen indépendant des actifs, des opérations ou de l'intégrité commerciale de votre organisation. Un audit des technologies de l'information (TI) examine spécifiquement les contrôles au sein des systèmes d'information de votre organisation. L'objectif d'un audit TI est de déterminer si les systèmes d'information fonctionnent efficacement, protègent les actifs et l'intégrité des données. Tous ces éléments sont importants pour répondre aux exigences réglementaires imposées par une norme ou un règlement de conformité.

Responsable de l'audit

Le terme propriétaire de l'audit a deux significations différentes selon le contexte.

Dans le contexte d'Audit Manager, le propriétaire d'un audit est un utilisateur ou un rôle gérant une évaluation et les ressources qui lui sont associées. Les responsabilités de ce persona au sein d'Audit Manager comprennent la création d'évaluations, l'examen des éléments probants et la génération de rapports d'évaluation. Audit Manager est un service collaboratif, et les propriétaires de l'audit bénéficient de la participation d'autres parties prenantes à leurs évaluations. Par exemple, vous pouvez ajouter d'autres propriétaires d'audit à votre évaluation pour partager les

tâches de gestion. Ou bien, si vous êtes propriétaire d'un audit et que vous avez besoin d'aide pour interpréter les éléments probants recueillis pour un contrôle, vous pouvez déléguer cet ensemble de contrôles à une partie prenante spécialisée dans ce domaine. Une telle personne est connue sous le nom de personne déléguée.

En termes commerciaux, le propriétaire d'un audit est une personne qui coordonne et supervise les efforts de préparation à l'audit de son entreprise et présente les éléments probants à un auditeur. Il s'agit généralement d'un professionnel de la gouvernance, gestion des risques et conformité (GRC), tel qu'un responsable de la conformité ou un responsable de la protection des données du RGPD. Les professionnels de la GRC ont l'expertise et l'autorité nécessaires pour gérer la préparation des audits. Plus précisément, ils comprennent les exigences de conformité et peuvent analyser, interpréter et préparer les données de rapport. Cependant, d'autres rôles commerciaux peuvent également assumer la persona de propriétaire d'audit dans Audit Manager. Les professionnels de la GRC ne sont pas les seuls à remplir ce rôle. Par exemple, vous pouvez choisir de faire configurer et gérer vos évaluations dans Audit Manager par un expert technique issu de l'une des équipes suivantes :

- SecOps
- INFORMATIQUE/ DevOps
- Centre des opérations de sécurité/réponse aux incidents
- Des équipes similaires qui possèdent, développent, corrigent et déploient des actifs dans le cloud et qui comprennent l'infrastructure cloud de votre organisation

La personne que vous choisissez de désigner en tant que propriétaire de l'audit dans le cadre de votre évaluation Audit Manager dépend en grande partie de votre organisation. Cela dépend également de la manière dont vous structurez vos opérations de sécurité et des spécificités de l'audit. Dans Audit Manager, la même personne peut assumer le rôle du propriétaire de l'audit dans une évaluation et celui de délégué dans une autre.

Quelle que soit la manière dont vous choisissez d'utiliser Audit Manager, vous pouvez gérer la séparation des tâches au sein de votre organisation en utilisant la persona de propriétaire ou délégué de l'audit et en accordant des politiques IAM spécifiques à chaque utilisateur. Grâce à cette approche en deux étapes, Audit Manager vous garantit un contrôle total sur tous les détails d'une évaluation individuelle. Pour plus d'informations, consultez Politiques recommandées pour les personas utilisateurs dans AWS Audit Manager.

AWS source gérée

Une source AWS gérée est une source de preuves qui AWS est conservée pour vous.

Chaque source AWS gérée est un groupe prédéfini de sources de données qui correspond à un contrôle commun ou à un contrôle central spécifique. Lorsque vous utilisez un contrôle commun comme source de preuves, vous collectez automatiquement des preuves pour tous les contrôles de base qui soutiennent ce contrôle commun. Vous pouvez également utiliser les contrôles de base individuels comme source de preuves.

Chaque fois qu'une source AWS gérée est mise à jour, les mêmes mises à jour sont automatiquement appliquées à tous les contrôles personnalisés qui utilisent cette source AWS gérée. Cela signifie que vos contrôles personnalisés collectent des preuves par rapport aux dernières définitions de cette source de preuves. Cela vous permet de garantir une conformité continue à mesure que l'environnement de conformité du cloud évolue.

Voir également :customer managed source,evidence source.

C

| B | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Journal des modifications

Pour chaque contrôle d'une évaluation, Audit Manager suit l'activité des utilisateurs pour ce contrôle. Vous pouvez ensuite consulter une piste d'audit des activités liées à un contrôle spécifique. Pour plus d'informations sur les activités des utilisateurs enregistrées dans le journal des modifications, consultez. Onglet Journal des modifications

Conformité dans le cloud

La conformité dans le cloud est le principe général selon lequel les systèmes fournis dans le cloud doivent être conformes aux normes auxquelles sont confrontés les clients de celui-ci.

Contrôle commun

veuillez consulter control.

Règlement de conformité

Un règlement de conformité est une loi, une règle ou un autre ordre prescrit par une autorité, généralement pour réglementer un comportement. Un exemple est le RGPD.

Norme de conformité

Une norme de conformité est un ensemble structuré de directives qui détaillent les processus d'une organisation dans le but de maintenir la conformité aux réglementations, spécifications ou lois établies. Des exemples incluent les normes PCI DSS et HIPAA.

Contrôle

Un contrôle est une sauvegarde ou une contre-mesure prescrite pour un système d'information ou une organisation. Les contrôles sont conçus pour protéger la confidentialité, l'intégrité et la disponibilité de vos informations, et pour répondre à un ensemble d'exigences définies. Ils garantissent que vos ressources fonctionnent comme prévu, que vos données sont fiables et que votre organisation respecte les lois et réglementations applicables.

Dans Audit Manager, un contrôle peut également représenter une question dans un questionnaire d'évaluation des risques liés aux fournisseurs. Dans ce cas, un contrôle est une question spécifique demandant des informations sur le niveau de sécurité et de conformité d'une organisation.

Les contrôles recueillent en permanence des éléments probants lorsqu'ils sont actifs dans vos évaluations d'Audit Manager. Vous pouvez également ajouter manuellement des éléments probants aux contrôles. Chaque élément de preuve est un dossier qui vous aide à démontrer la conformité aux exigences du contrôle.

Audit Manager fournit les types de contrôles suivants :

Type de commande	Description
Contrôle commun	Vous pouvez considérer un contrôle commun comme une action qui vous aide à atteindre un objectif de contrôle. Dans la mesure où les contrôles courants ne sont spécifiques à aucune norme de conformité, ils vous aident à collecter des preuves pouvant étayer une série d'obligations de conformité qui se chevauchent. Imaginons, par exemple, un objectif de contrôle appelé Classification et gestion des données. Pour atteindre cet objectif, vous pouvez mettre en œuvre un contrôle commun appelé contrôles d'accès pour surveiller et détecter les accès non autorisés à vos ressources.

Type de commande	Description
	• Les contrôles communs automatisés collectent des preuves pour vous. Ils consistent en un regroupement d'un ou de plusieurs contrôles de base connexes. À son tour, chacun de ces contrôles de base collecte automatiquement des preuves pertinentes à partir d'un groupe prédéfini de sources de AWS données. AWS gère ces sources de données sous-jacentes pour vous et les met à jour chaque fois que les réglementations et les normes changent et que de nouvelles sources de données sont identifiées. • Les contrôles manuels courants nécessitent que vous téléchargiez vos propres preuves. Cela s'explique par le fait qu'ils nécessitent généralement la fourniture d'enregistrements physiques ou de détails sur des événements qui se produisent en dehors de votre AWS environnement. Pour cette raison, il n'existe souvent aucune source de AWS données pouvant fournir des preuves à l'appui des exigences du contrôle commun manuel. Vous ne pouvez pas modifier un contrôle commun. Toutefois, vous pouvez utiliser n'importe quel contrôle commun comme source de preuves lorsque vous créez un contrôle personnalisé.

Type de commande	Description
Contrôle de base	Il s'agit d'une directive prescriptive pour votre AWS environnement. Vous pouvez considérer un contrôle de base comme une action qui vous aide à répondre aux exigences d'un contrôle commun. Supposons, par exemple, que vous utilisiez un contrôle courant appelé contrôles d'accès pour surveiller les accès non autorisés à vos ressources. Pour prendre en charge ce contrôle commun, vous pouvez utiliser le contrôle de base appelé Bloquer l'accès public en lecture dans les compartiments S3. Comme les contrôles de base ne sont spécifiques à aucune norme de conformité, ils collectent des preuves qui peuvent étayer une série d'obligat ions de conformité qui se chevauchent. Chaque contrôle de base utilise une ou plusieurs sources de données pour collecter des preuves concernant un élément spécifique Service AWS. AWS gère ces sources de données sous-jacentes pour vous et les met à jour chaque fois que les réglementations et les normes changent et que de nouvelles sources de données sont identifiées. Vous ne pouvez pas modifier un contrôle principal. Cependant, vous pouvez utiliser n'importe quel contrôle de base comme source de preuves lorsque vous créez un contrôle personnalisé.
Contrôle standard	Il s'agit d'un contrôle prédéfini fourni par Audit Manager. Vous pouvez utiliser les contrôles standard pour vous aider à préparer un audit pour une norme de conformité spécifique. Chaque contrôle standard est lié à une norme spécifique framework dans Audit Manager et collecte des preuves que vous pouvez utiliser pour démontrer la conformité à ce cadre. Les contrôles standard collectent des preuves à partir de sources de données sous-jacentes qui AWS gèrent. Ces sources de données sont automatiq uement mises à jour chaque fois que les réglementations et les normes changent et que de nouvelles sources de données sont identifiées. Vous ne pouvez pas modifier les commandes standard. Cependant, vous pouvez créer une copie modifiable de n'importe quel contrôle standard.

Type de commande	Description
Contrôle personnalisé	Il s'agit d'un contrôle que vous créez dans Audit Manager pour répondre à vos exigences de conformité spécifiques. Vous pouvez créer un contrôle personnalisé à partir de zéro ou créer une copie modifiable d'un contrôle standard existant. Lorsque vous créez un contrôle personnalisé, vous pouvez définir des paramètres spécifiques evidence source qui déterminent d'où Audit Manager collecte les preuves. Après avoir créé un contrôle personnalisé, vous pouvez le modifier ou l'ajouter à un cadre personnalisé. Vous pouvez également créer une copie modifiable de tout contrôle personnalisé.

Domaine de contrôle

Vous pouvez considérer un domaine de contrôle comme une catégorie de contrôles qui n'est spécifique à aucune norme de conformité. La protection des données est un exemple de domaine de contrôle.

Les contrôles sont souvent regroupés par domaine pour des raisons d'organisation simples. Chaque domaine a de multiples objectifs.

Les groupements de domaines de contrôle sont l'une des fonctionnalités les plus puissantes du tableau de bord d'Audit Manager. Audit Manager met en évidence les contrôles de vos évaluations qui contiennent des éléments probants non conformes et les regroupe par domaine de contrôle. Cela vous permet de concentrer vos efforts de remédiation sur des domaines spécifiques lorsque vous vous préparez à un audit.

Objectif de contrôle

Un objectif de contrôle décrit l'objectif des contrôles communs qui se situent en dessous de celui-ci. Chaque objectif peut avoir plusieurs contrôles communs. Si ces contrôles communs sont mis en œuvre avec succès, ils vous aideront à atteindre l'objectif.

Chaque objectif de contrôle relève d'un domaine de contrôle. Par exemple, le domaine de contrôle de la protection des données peut avoir un objectif de contrôle nommé Classification et traitement des données. Pour atteindre cet objectif de contrôle, vous pouvez utiliser un contrôle commun appelé contrôles d'accès pour surveiller et détecter les accès non autorisés à vos ressources.

Contrôle de base

veuillez consulter control.

Contrôle personnalisé

veuillez consulter control.

Source gérée par le client

Une source gérée par le client est une source de preuves que vous définissez.

Lorsque vous créez un contrôle personnalisé dans Audit Manager, vous pouvez utiliser cette option pour créer vos propres sources de données individuelles. Cela vous donne la flexibilité de collecter des preuves automatisées à partir d'une ressource spécifique à l'entreprise, telle qu'une règle personnalisée AWS Config . Vous pouvez également utiliser cette option si vous souhaitez ajouter des preuves manuelles à votre contrôle personnalisé.

Lorsque vous utilisez des sources gérées par le client, vous êtes responsable de la maintenance de toutes les sources de données que vous créez.

Voir également :AWS managed source,evidence source.

D

| B | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Source de données

Audit Manager utilise des sources de données pour collecter des preuves en vue d'un contrôle. Une source de données possède les propriétés suivantes :

- Un type de source de données définit le type de source de données à partir duquel Audit Manager collecte des preuves.
  - Pour les preuves automatisées, le type peut être AWS Security Hub, AWS Config AWS CloudTrail, ou des appels AWS d'API.
  - Si vous téléchargez vos propres preuves, le type est Manuel.
  - L'API Audit Manager désigne un type de source de données sous le nom de SourceType.
- Un mappage de source de données est un mot clé qui indique d'où proviennent les preuves pour un type de source de données donné.

  - Par exemple, il peut s'agir du nom d'un CloudTrail événement ou du nom d'une AWS Config règle.
  - L'API Audit Manager fait référence au mappage d'une source de données sous le nom de SourceKeyword.
- Le nom d'une source de données indique le couplage entre un type de source de données et le mappage.
  - Pour les contrôles standard, Audit Manager fournit un nom par défaut.
  - Pour les contrôles personnalisés, vous pouvez fournir votre propre nom.
  - L'API Audit Manager fait référence au nom d'une source de données sous le nom de sourceName.

Un seul contrôle peut avoir plusieurs types de sources de données et plusieurs mappages. Par exemple, un contrôle peut collecter des preuves à partir d'une combinaison de types de sources de données (tels que AWS Config Security Hub). Un autre contrôle peut avoir AWS Config comme seul type de source de données, avec plusieurs AWS Config règles sous forme de mappages.

Le tableau suivant répertorie les types de sources de données automatisées et présente des exemples de mappages correspondants.

Type de source de données	Description	Exemple de mappage
AWS Security Hub	Utilisez ce type de source de données pour obtenir un instantané de votre niveau de sécurité des ressources. Audit Manager utilise le nom d'un contrôle Security Hub comme mot-clé de mappage et communique le résultat de ce contrôle de sécurité directement depuis Security Hub.	`EC2.1`
AWS Config	Utilisez ce type de source de données pour obtenir un	`SNS_ENCRYPTED_KMS`

Type de source de données	Description	Exemple de mappage
	instantané de votre niveau de sécurité des ressources. Audit Manager utilise le nom d'une AWS Config règle comme mot-clé de mappage et rapporte le résultat de cette vérification de règle directement à partir de AWS Config.	
AWS CloudTrail	Utilisez ce type de source de données pour suivre une activité utilisateur spécifique nécessaire à votre audit. Audit Manager utilise le nom d'un CloudTrail événement comme mot-clé de mappage et collecte l'activité utilisate ur associée à partir de vos CloudTrail journaux.	`CreateAccessKey`
AWS Appels d'API	Utilisez ce type de source de données pour prendre un instantané de la configura tion de vos ressources par le biais d'un appel d'API à une source spécifique Service AWS. Audit Manager utilise le nom de l'appel d'API comme mot-clé de mappage et recueille la réponse de l'API.	`kms_ListKeys`

Délégué

Un délégué est un AWS Audit Manager utilisateur dont les autorisations sont limitées. Les délégués possèdent généralement une expertise commerciale ou technique spécialisée. Par exemple, cette expertise peut porter sur les politiques de conservation des données, les plans de formation, l'infrastructure réseau ou la gestion des identités. Les délégués aident les propriétaires de l'audit à examiner les éléments probants recueillis pour les contrôles relevant de leur domaine d'expertise. Les délégués peuvent examiner les ensembles de contrôles et les éléments probants associés, ajouter des commentaires, charger des éléments probants supplémentaires et mettre à jour le statut de chacun des contrôles que vous leur attribuez à des fins de révision.

Les propriétaires de l'audit attribuent des ensembles de contrôles spécifiques aux délégués, et non des évaluations complètes. Par conséquent, les délégués ont un accès limité aux évaluations. Pour obtenir des instructions sur la façon de déléguer un ensemble de contrôles, consultez Délégations en AWS Audit Manager.

E

| B | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Éléments probants

Un élément probant est un enregistrement qui contient les informations nécessaires pour démontrer la conformité aux exigences d'un contrôle. Des exemples d'éléments probants comprennent une activité de modification invoquée par un utilisateur et un instantané de la configuration du système.

Il existe deux principaux types d'éléments probants dans Audit Manager : les éléments probants automatisés et les éléments probants manuels.

Type de preuve	Description
Preuves automatisées	Il s'agit des preuves que l'Audit Manager collecte automatiquement. Ils comprennent les trois catégories d'éléments probants automatisés suivants : 1. Contrôle de conformité : le résultat d'un contrôle de conformité est capturé à partir de AWS Security Hub AWS Config, ou des deux.

Type de preuve	Description
	Parmi les exemples de contrôles de conformité, citons le résultat d'un contrôle de sécurité effectué par Security Hub pour un contrôle PCI DSS et une évaluation des AWS Config règles pour un contrôle HIPAA. Pour plus d'informations, consultez AWS Config Rules soutenu par AWS Audit Manager et AWS Security Hub commandes prises en charge par AWS Audit Manager. 2. Activité utilisateur — L'activité utilisateur qui modifie la configuration d'une ressource est capturée à partir des CloudTrail journaux au fur et à mesure que cette activité se produit. Des exemples d'activités des utilisateurs comprennent une mise à jour de la table de routage, une modification des paramètres de sauvegarde d'une instance Amazon RDS et une modification de la politique de chiffrement des compartiments S3. Pour plus d'informations, consultez AWS CloudTrail noms d'événements pris en charge par AWS Audit Manager. 3. Données de configuration : un instantané de la configuration des ressource s est capturé directement à partir d'un Service AWS sur une base quotidien ne, hebdomadaire ou mensuelle. Des exemples d'instantanés de configuration comprennent une liste de routes pour une table de routage VPC, un paramètre de sauvegarde d'instance Amazon RDS et une politique de chiffrement des compartiments S3. Pour plus d'informations, consultez AWS Appels d'API pris en charge par AWS Audit Manager.

Type de preuve	Description
Preuve manuelle	Il s'agit de la preuve que vous ajoutez vous-même à Audit Manager. Vous pouvez ajouter vos propres éléments probants de trois manières : 1. Importer un fichier à partir d'Amazon S3 2. Charger un fichier à partir de votre navigateur 3. Saisir une réponse textuelle à une question d'évaluation des risques Pour plus d'informations, consultez Ajouter des preuves manuelles dans AWS Audit Manager.

La collecte automatisée d'éléments probants débute lorsque vous créez une évaluation. Il s'agit d'un processus continu, et Audit Manager recueille des éléments probants à différentes fréquences en fonction du type d'éléments probants et de la source de données sous-jacente. Pour plus d'informations, consultez Comprendre le mode de AWS Audit Manager collecte des preuves.

Pour obtenir des instructions sur la façon d'examiner les éléments probants dans une évaluation, veuillez consulter Examen des preuves dans AWS Audit Manager.

Source de preuves

Une source de preuves définit l'endroit d'où un contrôle collecte des preuves. Il peut s'agir d'une source de données individuelle ou d'un groupe prédéfini de sources de données mappé à un contrôle commun ou à un contrôle central.

Lorsque vous créez un contrôle personnalisé, vous pouvez collecter des preuves auprès de sources AWS gérées, de sources gérées par le client, ou des deux.

> **Tip**
>
> Nous vous recommandons d'utiliser des sources AWS gérées. Chaque fois qu'une source AWS gérée est mise à jour, les mêmes mises à jour sont automatiquement appliquées à tous les contrôles personnalisés qui utilisent ces sources. Cela signifie que vos contrôles personnalisés collectent toujours des preuves par rapport aux dernières définitions de

cette source de preuves. Cela vous permet de garantir une conformité continue à mesure que l'environnement de conformité du cloud évolue.

Voir également :AWS managed source,customer managed source.

Méthode de collecte d'éléments probants

Un contrôle peut recueillir des éléments probants de deux manières.

Méthode de collecte d'éléments probants	Description
Automatisé	Les contrôles automatisés collectent automatiquement des preuves à partir de sources de AWS données. Ces éléments probants automatisés peuvent vous aider à démontrer la conformité totale ou partielle envers le contrôle.
Manuel	Les contrôles manuels nécessitent que vous téléchargiez vos propres preuves pour démontrer la conformité au contrôle.

> **Note**
>
> Vous pouvez joindre des éléments probants manuels à tout contrôle automatisé. Dans de nombreux cas, il est nécessaire d'avoir une combinaison d'éléments probants automatisés et manuels pour démontrer la conformité totale envers un contrôle. Bien qu'Audit Manager puisse fournir des éléments probants automatisés utiles et pertinents, certains éléments probants automatisés peuvent ne démontrer qu'une conformité partielle. Dans ce cas, vous pouvez compléter les éléments probants automatisés fournies par Audit Manager avec vos propres éléments probants.
> Par exemple :
>
> - AWS cadre des meilleures pratiques d'IA générative v2Il contient un contrôle appelé`Error analysis`. Ce contrôle vous oblige à identifier les cas de détection d'inexactitudes dans l'utilisation de votre modèle. Cela vous oblige également à effectuer une analyse approfondie des erreurs afin d'en comprendre les causes profondes et d'entreprendre des mesures correctives.

- Pour soutenir ce contrôle, Audit Manager collecte des preuves automatisées qui indiquent si les CloudWatch alarmes sont activées pour l' Compte AWS endroit où votre évaluation est en cours d'exécution. Vous pouvez utiliser ces éléments probants pour démontrer une conformité partielle avec le contrôle en prouvant que vos alarmes et contrôles sont configurés correctement.
- Pour démontrer une conformité totale, vous pouvez compléter les éléments probants automatisés avec des éléments probants manuels. Par exemple, vous pouvez charger une politique ou une procédure qui indique votre processus d'analyse des erreurs, vos seuils pour les escalades et les rapports, ainsi que les résultats de votre analyse des causes profondes. Vous pouvez utiliser ces éléments probants manuels pour démontrer que les politiques établies sont en place et que des mesures correctives ont été prises lorsque cela vous a été demandé.

Pour un exemple plus détaillé, veuillez consulter la section Contrôles avec sources de données mixtes.

Destination d'exportation

Une destination d'exportation est le compartiment S3 par défaut dans lequel Audit Manager enregistre les fichiers que vous exportez depuis la recherche d'éléments probants. Pour plus d'informations, consultez Configuration de votre destination d'exportation par défaut pour Evidence Finder.

F

| B | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Framework

Un cadre d'Audit Manager structure et automatise les évaluations pour une norme spécifique ou un principe de gouvernance des risques. Ces frameworks incluent un ensemble de contrôles prédéfinis ou définis par le client, et ils vous aident à adapter vos AWS ressources aux exigences de ces contrôles.

Il existe deux types de framework dans Audit Manager.

Type de cadre	Description
Cadre standard	Il s'agit d'un cadre prédéfini basé sur les AWS meilleures pratiques relatives à diverses normes et réglementations de conformité. Vous pouvez utiliser des cadres standard pour vous aider à préparer les audits pour une norme ou une réglementation de conformité spécifique, telle que la norme PCI DSS ou la loi HIPAA.
Framework personnalisé	Il s'agit d'un framework personnalisé que vous définissez en tant qu'utilis ateur d'Audit Manager. Vous pouvez utiliser des cadres personnalisés pour vous aider à préparer l'audit en fonction de vos exigences spécifiques en matière de GRC.

Pour voir les instructions de création et de gestion des frameworks, veuillez consulter Utilisation de la bibliothèque de frameworks pour gérer les frameworks dans AWS Audit Manager.

> **Note**
>
> AWS Audit Manager aide à recueillir des preuves pertinentes pour vérifier la conformité aux normes et réglementations de conformité spécifiques. Cependant, il n'évalue pas votre conformité lui-même. Les preuves collectées par ce biais peuvent AWS Audit Manager donc ne pas inclure toutes les informations relatives à votre AWS utilisation nécessaires aux audits. AWS Audit Manager ne remplace pas un conseiller juridique ou un expert en conformité.

Partage de frameworks

Vous pouvez utiliser Partage d'un framework personnalisé dans AWS Audit Manager cette fonctionnalité pour partager rapidement vos frameworks personnalisés entre Comptes AWS les régions. Pour partager un framework personnalisé, vous devez créer une demande de partage. Le destinataire dispose alors de 120 jours pour accepter ou refuser la demande. Lorsqu'il accepte la demande de partage, Audit Manager reproduit le framework personnalisé partagé dans sa bibliothèque de frameworks. Outre la réplication du framework personnalisé, Audit Manager reproduit également tous les ensembles de contrôles personnalisés et les contrôles personnalisés

contenus dans ce framework. Ces contrôles personnalisés sont ajoutés à la bibliothèque de contrôles du destinataire. Audit Manager ne réplique pas les frameworks ou les contrôles standard. Cela est dû au fait que ces ressources sont déjà disponibles par défaut dans chaque compte et région.

R

| B | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Ressource

Une ressource est un actif physique ou informationnel évalué dans le cadre d'un audit. Les exemples de AWS ressources incluent les instances Amazon EC2, les instances Amazon RDS, les compartiments Amazon S3 et les sous-réseaux Amazon VPC.

Évaluation des ressources

L'évaluation des ressources est le processus d'évaluation d'une ressource individuelle. Cette évaluation est basée sur l'exigence d'un contrôle. Lorsqu'une évaluation est active, Audit Manager effectue des évaluations des ressources pour chaque ressource individuelle comprise dans le cadre de l'évaluation. Une évaluation des ressources exécute les tâches suivantes :

1. Recueille des éléments probants, notamment les configurations des ressources, les journaux d'événements et les résultats
2. Traduit et mappe les éléments probants sur les contrôles
3. Stocke et suit la lignée des éléments probants pour garantir l'intégrité

Conformité des ressources

La conformité des ressources fait référence au statut d'évaluation d'une ressource qui a été évaluée lors de la collecte d'éléments probants pour la vérification de conformité.

Audit Manager collecte des preuves de conformité pour les contrôles qui utilisent AWS Config Security Hub comme type de source de données. Plusieurs ressources peuvent être évaluées au cours de cette collecte d'éléments probants. Par conséquent, un même élément probant pour la vérification de conformité peut comprendre une ou plusieurs ressources.

Vous pouvez utiliser le filtre de conformité des ressources dans la recherche d'éléments probants pour explorer l'état de conformité au niveau des ressources. Une fois votre requête de recherche terminée, vous pouvez prévisualiser les ressources qui lui correspondent.

Dans la recherche d'éléments probants, il existe trois valeurs possibles pour la conformité des ressources :

Valeur	Description
Non conforme	Cela fait référence aux ressources présentant des problèmes de contrôle de conformité. Cela se produit si Security Hub signale un résultat d'échec pour la ressource ou s'il AWS Config signale un résultat non conforme.
Conforme	Cela fait référence aux ressources qui ne présentent aucun problème de contrôle de conformité. Cela se produit si Security Hub indique un résultat de réussite pour la ressource, ou s'il AWS Config indique un résultat conforme.
Peu concluant	Cela fait référence aux ressources pour lesquelles aucun contrôle de conformité n'est disponible ou applicable. Cela se produit si AWS Config Security Hub est le type de source de données sous-jacent, mais que ces services ne sont pas activés. Cela se produit également si le type de source de données sous-jacent ne prend pas en charge les contrôles de conformité (tels que les preuves manuelles, les appels d' AWS API ou CloudTrail).

S

| B | | | | G | H | I | J | K | L | M | N | O | P | Q | | | T | U | V | W | X | Y | Z

Service inclus

Audit Manager gère Services AWS les domaines concernés par vos évaluations. Si vous avez une évaluation plus ancienne, il est possible que vous ayez spécifié manuellement les services concernés par le passé. Après le 4 juin 2024, vous ne pourrez plus spécifier ou modifier manuellement les services concernés.

Un service inclus dans le champ d'application est un service pour Service AWS lequel votre évaluation recueille des preuves. Lorsqu'un service est inclus dans le périmètre de votre évaluation, Audit Manager évalue les ressources de ce service. Quelques exemples de ressources possibles :

- Instance Amazon EC2
- Compartiment S3
- Un utilisateur ou un rôle IAM
- Table DynamoDB
- Composant réseau tel qu'un cloud privé virtuel (VPC) d'Amazon, un groupe de sécurité ou une table de liste de contrôle d'accès (ACL) au réseau

Par exemple, si Amazon S3 est un service concerné, Audit Manager peut collecter des preuves concernant vos compartiments S3. Les preuves exactes collectées sont déterminées par celles d'un contrôledata source. Par exemple, si le type de source de données est AWS Config et que le mappage des sources de données est une AWS Config règle (telle que`s3-bucket-public-write-prohibited`), Audit Manager collecte le résultat de cette évaluation des règles à titre de preuve.

> **Note**
>
> N'oubliez pas qu'un service concerné est différent d'un type de source de données, qui peut également être un Service AWS ou autre. Pour plus d'informations, consultez Quelle est la différence entre un service concerné et un type de source de données ? la section Dépannage de ce guide.

Contrôle standard

veuillez consulter control.

Comprendre le mode de AWS Audit Manager collecte des preuves

Chaque évaluation active collecte AWS Audit Manager automatiquement des preuves à partir de diverses sources de données. Dans chaque évaluation, vous définissez le responsable de l' Comptes AWS audit qui collectera les preuves, et le responsable de l'audit gère Services AWS les éléments concernés. Chacun de ces services et comptes contient plusieurs ressources que vous

possédez et utilisez. La collecte d'éléments probants dans Audit Manager implique l'évaluation de chaque ressource concernée. C'est ce que l'on appelle une évaluation des ressources.

Les étapes suivantes décrivent la manière dont Audit Manager recueille les éléments probants pour chaque évaluation des ressources :

1. Évaluation d'une ressource à partir de la source de données

Pour commencer à recueillir des éléments probants, Audit Manager évalue une ressource concernée à partir d'une source de données. Pour ce faire, il capture un instantané de configuration, le résultat d'un contrôle de conformité associé ou l'activité de l'utilisateur. Il exécute ensuite une analyse pour déterminer le contrôle pris en charge par ces données. Le résultat de l'évaluation des ressources est ensuite enregistré et converti en éléments probants. Pour plus d'informations sur les différents types de preuves, consultez evidence la section de ce guide consacrée aux AWS Audit Manager concepts et à la terminologie.

2. Conversion des résultats d'évaluation en éléments probants

Le résultat de l'évaluation des ressources contient à la fois les données d'origine capturées à partir de cette ressource et les métadonnées indiquant le contrôle pris en charge par les données. Audit Manager convertit les données d'origine dans un format convivial pour les auditeurs. Les données et métadonnées converties sont ensuite enregistrées en tant qu'éléments probants pour Audit Manager avant d'être associées à un contrôle.

3. Lien des éléments probants au contrôle correspondant

Audit Manager lit les métadonnées des éléments probants. Ensuite, il joint les éléments probants enregistrés à un contrôle associé dans le cadre de l'évaluation. Les éléments probants joints deviennent visibles dans Audit Manager. Le cycle d'une évaluation des ressources s'achève ainsi.

> **Note**
>
> Selon les configurations de contrôle, les mêmes éléments probants peuvent, dans certains cas, être joints à plusieurs contrôles issus de plusieurs évaluations d'Audit Manager. Lorsque les mêmes éléments probants sont joints à plusieurs contrôles, Audit Manager mesure une seule fois l'évaluation des ressources. Cela s'explique par le fait que les mêmes éléments probants ne sont recueillies qu'une seule fois. Cependant, dans le cadre d'une évaluation Audit Manager, un contrôle peut contenir plusieurs éléments probants provenant de plusieurs sources de données.

Fréquence de collecte des éléments probants

La collecte d'éléments probants est un processus continu et commence lorsque vous créez votre évaluation. Audit Manager collecte des preuves provenant de plusieurs sources de données à des fréquences variables. Par conséquent, il n'y a pas de one-size-fits-all réponse quant à la fréquence à laquelle les preuves sont collectées. La fréquence de collecte des éléments probants est basée sur le type d'élément probant et sa source de données, comme décrit ci-dessous.

- Contrôles de conformité — Audit Manager collecte ce type de preuves auprès de AWS Security Hub et AWS Config.
  - Pour Security Hub, la collecte de preuves suit le calendrier de vos contrôles Security Hub. Pour plus d'informations sur le calendrier des vérifications du Security Hub, veuillez consulter la section Planification de l'exécution des contrôles de sécurité dans le Guide de l'utilisateur AWS Security Hub . Pour plus d'informations sur les vérifications de Security Hub pris en charge par Audit Manager, veuillez consulter AWS Security Hub commandes prises en charge par AWS Audit Manager.
  - En AWS Config effet, la collecte de preuves suit les déclencheurs définis dans vos AWS Config règles. Pour plus d'informations sur les déclencheurs des règles AWS Config , veuillez consulter la section Types de déclencheurs dans le Guide de l'utilisateur AWS Config . Pour plus d'informations sur ceux AWS Config Rules pris en charge par Audit Manager, consultezAWS Config Rules soutenu par AWS Audit Manager.
- Activité des utilisateurs — Audit Manager collecte ce type de AWS CloudTrail preuves de manière continue. Cette fréquence est continue car l'activité utilisateur peut se produire à tout moment de la journée. Pour plus d'informations, consultez AWS CloudTrail noms d'événements pris en charge par AWS Audit Manager.
- Données de configuration : Audit Manager collecte ce type de preuve à l'aide d'un appel d'API de description envoyé à un autre opérateur Service AWS tel qu'Amazon EC2, Amazon S3 ou IAM. Vous pouvez choisir quelles actions d'API appeler. Vous pouvez également définir la fréquence sur quotidienne, hebdomadaire ou mensuelle dans Audit Manager. Vous pouvez la spécifier lorsque vous créez ou modifiez un contrôle dans la bibliothèque de contrôles. Pour voir les instructions d'édition et de création des contrôles, veuillez consulter Utilisation de la bibliothèque de commandes pour gérer les commandes dans AWS Audit Manager. Pour plus d'informations sur les appels d'API pris en charge par Audit Manager, consultezAWS Appels d'API pris en charge par AWS Audit Manager.

Quelle que soit la fréquence de collecte des éléments probants pour la source de données, les nouveaux éléments probants sont recueillis automatiquement tant que le contrôle et l'évaluation sont actifs.

Exemples de AWS Audit Manager contrôles

Sur cette page, vous pouvez consulter des exemples pour en découvrir plus sur le fonctionnement des contrôles dans AWS Audit Manager.

Dans Audit Manager, les contrôles peuvent collecter automatiquement des preuves à partir de quatre types de sources de données :

1. AWS CloudTrail— Capturez l'activité des utilisateurs à partir de vos CloudTrail journaux et importez-la comme preuve de l'activité des utilisateurs
2. AWS Security Hub— Collectez les résultats depuis Security Hub et importez-les comme preuves de contrôle de conformité
3. AWS Config— Collectez des évaluations de règles AWS Config et importez-les comme preuves de contrôle de conformité
4. AWS Appels d'API — Capturez un instantané des ressources à partir d'un appel d'API et importez-le en tant que preuve des données de configuration

De nombreux contrôles collectent des preuves à l'aide de groupements prédéfinis de ces sources de données. Ces groupements de sources de données sont appelés sources AWS gérées. Chaque source AWS gérée représente un contrôle commun ou un contrôle de base. Cela vous permet de mapper efficacement vos exigences de conformité à un groupe pertinent de sources de données validées et gérées par des évaluateurs certifiés par le secteur. AWS Vous pouvez également utiliser les quatre types de sources de données ci-dessus pour définir vos propres sources de données. Cela vous donne la flexibilité de télécharger des preuves manuelles ou de collecter des preuves automatisées à partir d'une ressource spécifique à l'entreprise, telle qu'une règle personnalisée AWS Config .

Les exemples de cette page montrent comment les contrôles collectent des preuves à partir de chacun des types de sources de données individuels. Ils décrivent à quoi ressemble un contrôle, comment Audit Manager collecte les preuves à partir de la source de données et les prochaines étapes à suivre pour démontrer la conformité.

> **Tip**
>
> Nous vous recommandons d'activer AWS Config Security Hub pour une expérience optimale dans Audit Manager. Lorsque vous activez ces services, Audit Manager peut utiliser les résultats du Security Hub et AWS Config Rules générer des preuves automatisées.
>
> - Une fois que vous avez activé AWS Security Hub, assurez-vous d'activer également toutes les normes de sécurité et d'activer le paramètre des résultats de contrôle consolidés. Cette étape permet à Audit Manager d'importer les résultats correspondant à toutes les normes de conformité prises en charge.
> - Après avoir activé AWS Config, assurez-vous d'activer également le pack de conformité approprié AWS Config Rules ou de déployer un pack de conformité pour la norme de conformité liée à votre audit. Cette étape garantit qu'Audit Manager peut importer les résultats pour tous les supports AWS Config Rules que vous avez activés.

Des exemples sont disponibles pour chacun des types de contrôles suivants :

Rubriques

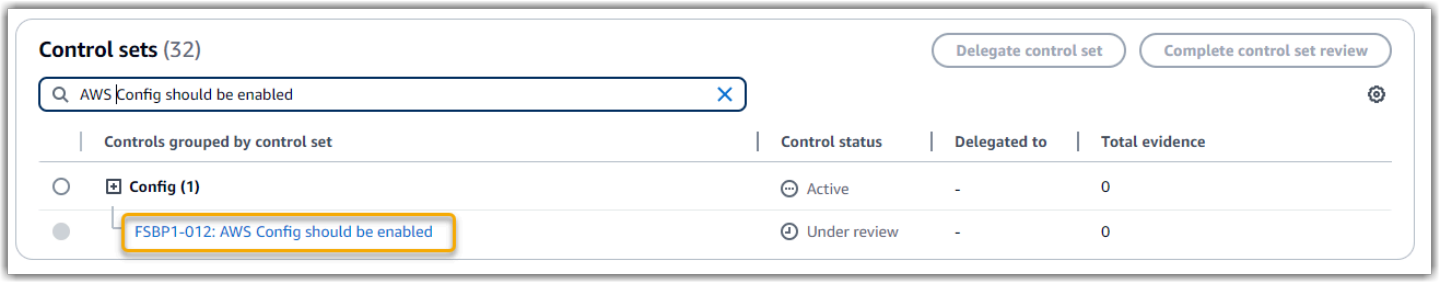
Contrôles automatisés utilisés AWS Security Hub comme type de source de données

Cet exemple montre un contrôle utilisé AWS Security Hub comme type de source de données. Il s'agit d'un contrôle standard issu du AWS framework Bonnes pratiques de sécurité de base (FSBP, Foundational Security Best Practices). Audit Manager utilise ce contrôle pour générer des preuves qui peuvent aider à mettre votre AWS environnement en conformité avec les exigences du FSBP.

Exemple de détails de contrôle

- Nom du contrôle : `FSBP1-012: AWS Config should be enabled`
- Kit de commande —`Config`. Il s'agit d'un regroupement spécifique au framework de contrôles FSBP liés à la gestion de la configuration.
- Source de preuves — Sources de données individuelles
- Type de source de données : AWS Security Hub
- Type d'élément probant : vérification de conformité

Dans l'exemple suivant, ce contrôle fait partie d'une évaluation Audit Manager créée à partir du framework FSBP.



L'évaluation indique l'état du contrôle. Il montre également la quantité de preuves recueillies pour ce contrôle jusqu'à présent. À partir de là, vous pouvez déléguer l'ensemble de contrôles à des fins de révision ou l'effectuer vous-même. Le choix du nom du contrôle ouvre une page de détails contenant plus d'informations, y compris les éléments probants de ce contrôle.

Ce que réalise ce contrôle

Ce contrôle nécessite qu' AWS Config il soit activé partout Régions AWS où vous utilisez Security Hub. Audit Manager peut utiliser ce contrôle pour vérifier si vos politiques IAM sont trop larges pour répondre aux exigences du FSBP. Plus précisément, il peut vérifier si les politiques IAM gérées par le client disposent d'un accès administrateur comprenant l'instruction générique suivante : `"Effect": "Allow"` avec `"Action": "*"` sur `"Resource": "*"`.

Fonctionnement de la collecte des éléments probants par Audit Manager pour ce contrôle

Audit Manager prend les mesures suivantes pour recueillir les éléments probants pour ce contrôle :

1. Pour chaque contrôle, Audit Manager évalue vos ressources concernées. Pour ce faire, il utilise la source de données spécifiée dans les paramètres de contrôle. Dans cet exemple, vos politiques

IAM sont la ressource, et Security Hub est le type de source de données. AWS Config Audit Manager recherche le résultat d'une vérification spécifique du Security Hub ([IAM.1]), qui utilise à son tour une AWS Config règle pour évaluer vos politiques IAM (iam-policy-no-statements-). with-admin-access

2. Le résultat de l'évaluation des ressources est enregistré et converti en éléments probants conviviaux pour l'auditeur. Audit Manager génère des éléments probants pour la vérification de conformité pour les contrôles qui utilisent Security Hub comme type de source de données. Ces éléments probants contiennent le résultat de la vérification de conformité signalé directement depuis Security Hub.
3. Audit Manager joint les éléments probants enregistrés au contrôle nommé `FSBP1-012: AWS Config should be enabled` dans votre évaluation.

Comment utiliser Audit Manager pour démontrer la conformité à ce contrôle

Une fois les éléments probants joints au contrôle, vous (ou un délégué de votre choix) pouvez les examiner pour déterminer si des mesures correctives sont nécessaires.

Dans cet exemple, Audit Manager peut afficher une décision d'échec émanant de Security Hub. Cela peut se produire si vos politiques IAM contiennent des caractères génériques (*) et sont trop larges pour répondre au contrôle. Dans ce cas, vous pouvez mettre à jour vos politiques IAM afin qu'elles n'accordent pas de privilèges administratifs complets. Pour ce faire, vous pouvez déterminer quelles tâches doivent effectuer les utilisateurs, puis élaborer des stratégies leur permettant de réaliser uniquement ces tâches. Cette action corrective permet de mettre votre AWS environnement en conformité avec les exigences du FSBP.

Lorsque vos politiques IAM sont conformes au contrôle, indiquez ce dernier comme étant examiné et ajoutez les éléments probants à votre rapport d'évaluation. Vous pouvez ensuite partager ce rapport avec les auditeurs pour démontrer que le contrôle fonctionne comme prévu.

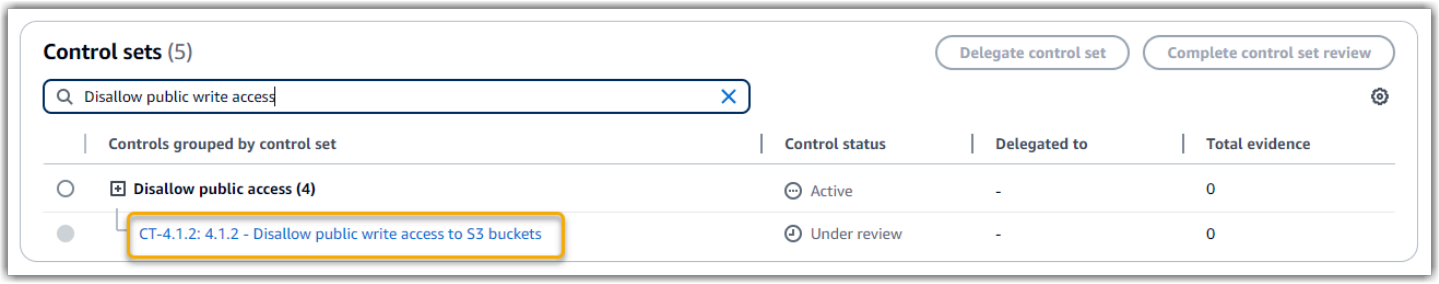
Contrôles automatisés utilisés AWS Config comme type de source de données

Cet exemple montre un contrôle utilisé AWS Config comme type de source de données. Il s'agit d'un contrôle standard issu du framework de barrière de protection AWS Control Tower. Audit Manager utilise ce contrôle pour générer des preuves qui aident à aligner votre AWS environnement sur AWS Control Tower Guardrails.

Exemple de détails de contrôle

- Nom du contrôle : `CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets`
- Ensemble de contrôles : ce contrôle appartient à l'ensemble de contrôles `Disallow public access`. Il s'agit d'un groupe de contrôles liés à la gestion des accès.
- Source de preuves — Sources de données individuelles
- Type de source de données : AWS Config
- Type d'élément probant : vérification de conformité

Dans l'exemple suivant, ce contrôle fait partie d'une évaluation Audit Manager créée à partir du framework AWS Control Tower Guardrails.



L'évaluation indique l'état du contrôle. Il montre également la quantité de preuves recueillies pour ce contrôle jusqu'à présent. À partir de là, vous pouvez déléguer l'ensemble de contrôles à des fins de révision ou l'effectuer vous-même. Le choix du nom du contrôle ouvre une page de détails contenant plus d'informations, y compris les éléments probants de ce contrôle.

Ce que réalise ce contrôle

Audit Manager peut utiliser ce contrôle pour vérifier si les niveaux d'accès de vos politiques de compartiment S3 sont trop indulgents pour répondre aux AWS Control Tower exigences. Plus précisément, il peut vérifier les paramètres de blocage de l'accès public, les politiques relatives aux compartiments et les listes de contrôle d'accès (ACL) à ceux-ci pour confirmer qu'ils n'autorisent pas l'accès public en écriture.

Fonctionnement de la collecte des éléments probants par Audit Manager pour ce contrôle

Audit Manager prend les mesures suivantes pour recueillir les éléments probants pour ce contrôle :

1. Pour chaque contrôle, Audit Manager évalue vos ressources concernées à l'aide de la source de données spécifiée dans les paramètres du contrôle. Dans ce cas, vos compartiments S3

constituent la ressource et AWS Config est le type de source de données. Audit Manager recherche le résultat d'une AWS Config règle spécifique (s3- bucket-public-write-prohibited) pour évaluer les paramètres, la politique et l'ACL de chacun des compartiments S3 concernés par votre évaluation.

2. Le résultat de l'évaluation des ressources est enregistré et converti en éléments probants conviviaux pour l'auditeur. Audit Manager génère des preuves de contrôle de conformité pour les contrôles utilisés AWS Config comme type de source de données. Ces preuves contiennent le résultat du contrôle de conformité rapporté directement auprès de AWS Config.
3. Audit Manager joint les éléments probants enregistrés au contrôle nommé `CT-4.1.2: 4.1.2 - Disallow public write access to S3 buckets` dans votre évaluation.

Comment utiliser Audit Manager pour démontrer la conformité à ce contrôle

Une fois les éléments probants joints au contrôle, vous (ou un délégué de votre choix) pouvez les examiner pour déterminer si des mesures correctives sont nécessaires.

Dans cet exemple, Audit Manager peut afficher une décision AWS Config indiquant qu'un compartiment S3 n'est pas conforme. Cela peut se produire si l'un de vos compartiments S3 possède un paramètre de blocage de l'accès public qui ne restreint pas les politiques publiques, et si la politique utilisée autorise l'accès public en écriture. Pour remédier à ce problème, vous pouvez mettre à jour le paramètre de blocage de l'accès public afin de restreindre les politiques publiques. Vous pouvez également utiliser une autre politique de compartiment qui n'autorise pas l'accès public en écriture. Cette action corrective permet de mettre votre AWS environnement en conformité avec AWS Control Tower les exigences.

Lorsque vous êtes certain que les niveaux d'accès à votre compartiment S3 sont conformes au contrôle, vous pouvez l'indiquer comme examiné et ajouter les éléments probants à votre rapport d'évaluation. Vous pouvez ensuite partager ce rapport avec les auditeurs pour démontrer que le contrôle fonctionne comme prévu.

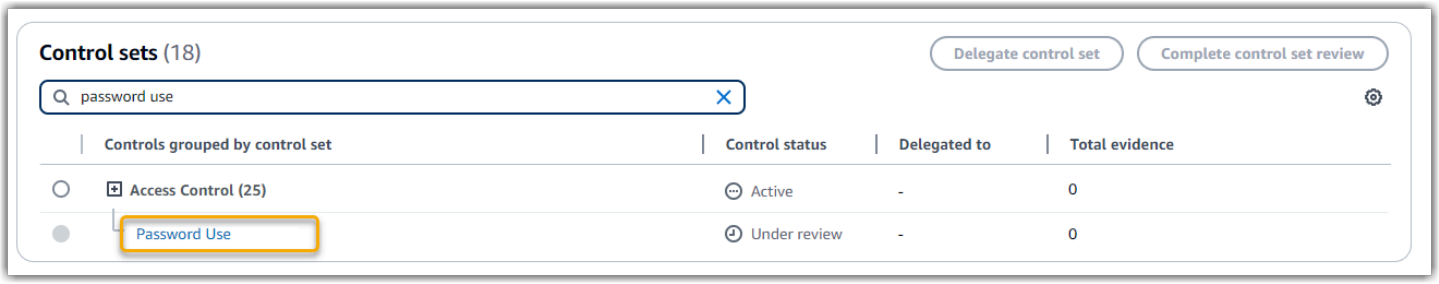
Contrôles automatisés utilisant les appels AWS d'API comme type de source de données

Cet exemple montre un contrôle personnalisé qui utilise des appels AWS d'API comme type de source de données. Audit Manager utilise ce contrôle pour générer des preuves qui peuvent aider à AWS adapter votre environnement à vos exigences spécifiques.

Exemple de détails de contrôle

- Nom du contrôle : `Password Use`
- Ensemble de contrôles : ce contrôle appartient à un ensemble de contrôles appelé `Access Control`. Il s'agit d'un groupe de contrôles liés à la gestion des identités et des accès.
- Source de preuve — Source de données individuelle
- Type de source de données : appels AWS d'API
- Type d'éléments probants : données de configuration

Dans l'exemple suivant, ce contrôle fait partie d'une évaluation Audit Manager créée à partir d'un framework personnalisé.



L'évaluation indique l'état du contrôle. Il montre également la quantité de preuves recueillies pour ce contrôle jusqu'à présent. À partir de là, vous pouvez déléguer l'ensemble de contrôles à des fins de révision ou l'effectuer vous-même. Le choix du nom du contrôle ouvre une page de détails contenant plus d'informations, y compris les éléments probants de ce contrôle.

Ce que réalise ce contrôle

Audit Manager peut utiliser ce contrôle personnalisé pour vous aider à garantir que vous avez mis en place des politiques de contrôle d'accès suffisantes. Il nécessite que vous suiviez les bonnes pratiques de sécurité lors de la sélection et de l'utilisation des mots de passe. Audit Manager peut vous aider à le valider en récupérant une liste de toutes les politiques de mot de passe pour les principaux IAM concernés par votre évaluation.

Fonctionnement de la collecte des éléments probants par Audit Manager pour ce contrôle

Audit Manager prend les mesures suivantes pour recueillir les éléments probants pour ce contrôle personnalisé :

1. Pour chaque contrôle, Audit Manager évalue vos ressources concernées à l'aide de la source de données spécifiée dans les paramètres du contrôle. Dans ce cas, vos principaux IAM sont

les ressources, et les appels d' AWS API sont le type de source de données. Audit Manager recherche le résultat d'un appel d'API IAM spécifique (GetAccountPasswordPolicy). Il renvoie ensuite les politiques relatives aux mots de passe pour les Comptes AWS qui entrent dans le cadre de votre évaluation.

2. Le résultat de l'évaluation des ressources est enregistré et converti en éléments probants conviviaux pour l'auditeur. Audit Manager génère des éléments probants de données de configuration pour les contrôles qui utilisent des appels d'API en tant que source de données. Ces éléments probants contiennent les données d'origine capturées à partir des réponses de l'API, ainsi que des métadonnées supplémentaires indiquant le contrôle pris en charge par les données.
3. Audit Manager joint les éléments probants enregistrés au contrôle personnalisé nommé `Password Use` dans votre évaluation.

Comment utiliser Audit Manager pour démontrer la conformité à ce contrôle

Une fois les éléments probants joints au contrôle, vous (ou un délégué de votre choix) pouvez les examiner pour déterminer s'ils sont suffisants ou si des mesures correctives sont nécessaires.

Dans cet exemple, vous pouvez examiner les éléments probants pour voir les réponses de l'appel d'API. La GetAccountPasswordPolicyréponse décrit les exigences de complexité et les périodes de rotation obligatoires pour les mots de passe utilisateur de votre compte. Vous pouvez utiliser cette réponse de l'API comme preuve pour démontrer que vous avez mis en place des politiques de contrôle d'accès par mot de Comptes AWS passe suffisantes pour les objectifs visés par votre évaluation. Si vous le souhaitez, vous pouvez également fournir des commentaires supplémentaires sur ces politiques en ajoutant un commentaire au contrôle.

Lorsque vous êtes certain que les politiques de mots de passe de vos principaux IAM sont conformes au contrôle personnalisé, vous pouvez marquer le contrôle comme examiné et ajouter les éléments probants à votre rapport d'évaluation. Vous pouvez ensuite partager ce rapport avec les auditeurs pour démontrer que le contrôle fonctionne comme prévu.

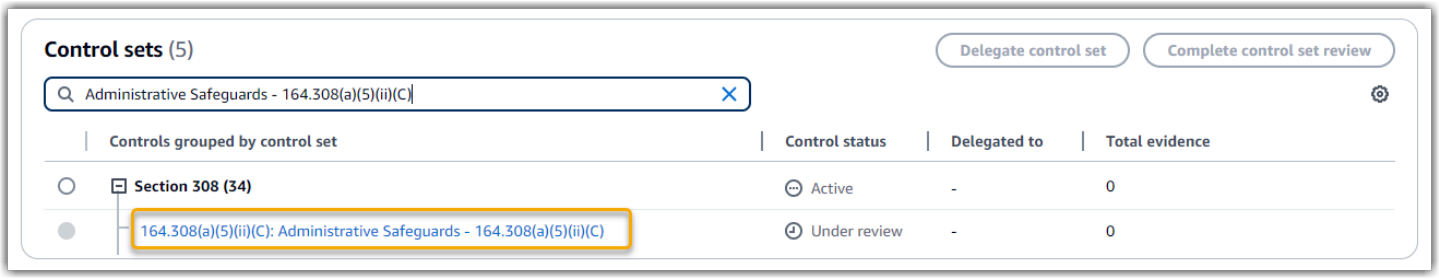
Contrôles automatisés utilisés AWS CloudTrail comme type de source de données

Cet exemple montre un contrôle utilisé AWS CloudTrail comme type de source de données. Il s'agit d'un contrôle standard issu du framework HIPAA Security Rule 2003. Audit Manager utilise ce contrôle pour générer des éléments probants qui peuvent aider à mettre votre environnement AWS en conformité avec les exigences HIPAA.

Exemple de détails de contrôle

- Nom du contrôle : `164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C)`
- Ensemble de contrôles : ce contrôle appartient à l'ensemble de contrôles appelé `Section 308`. Il s'agit d'un regroupement spécifique au cadre de contrôles HIPAA relatifs aux garanties administratives.
- Source de preuves — source AWS gérée (contrôles de base)
- Type de source de données sous-jacente : AWS CloudTrail
- Type d'éléments probants : activité utilisateur

Voici ce contrôle présenté dans le cadre d'une évaluation d'Audit Manager créée à partir du framework HIPAA :



L'évaluation indique l'état du contrôle. Il montre également la quantité de preuves recueillies pour ce contrôle jusqu'à présent. À partir de là, vous pouvez déléguer l'ensemble de contrôles à des fins de révision ou l'effectuer vous-même. Le choix du nom du contrôle ouvre une page de détails contenant plus d'informations, y compris les éléments probants de ce contrôle.

Ce que réalise ce contrôle

Ce contrôle nécessite la mise en place de procédures de surveillance pour détecter les accès non autorisés. Un exemple d'accès non autorisé est celui où une personne se connecte à la console sans que l'authentification multifactorielle (MFA) soit activée. Audit Manager vous aide à valider ce contrôle en fournissant la preuve que vous avez configuré Amazon pour surveiller les demandes de connexion CloudWatch à la console de gestion lorsque le MFA n'est pas activé.

Fonctionnement de la collecte des éléments probants par Audit Manager pour ce contrôle

Audit Manager prend les mesures suivantes pour recueillir les éléments probants pour ce contrôle :

1. Pour chaque contrôle, Audit Manager évalue les ressources concernées à l'aide des sources de preuves spécifiées dans les paramètres de contrôle. Dans ce cas, le contrôle utilise plusieurs contrôles de base comme sources de preuves.

   Chaque contrôle de base est un regroupement géré de sources de données individuelles. Dans notre exemple, l'un de ces contrôles de base (`Configure Amazon CloudWatch alarms to detect management console sign-in requests without MFA enabled`) est utilisé CloudTrail comme source de données. CloudTrail est le type de source de données, et les CloudWatch alarmes Amazon sont la ressource évaluée.

   Audit Manager examine vos CloudTrail journaux en utilisant le `monitoring_EnableAlarmActions` mot clé pour trouver les actions activant les CloudWatch alarmes enregistrées par CloudTrail. Il renvoie ensuite un journal des événements pertinents entrant dans le cadre de votre évaluation.
2. Le résultat de l'évaluation des ressources est enregistré et converti en éléments probants conviviaux pour l'auditeur. Audit Manager génère des preuves de l'activité des utilisateurs pour les contrôles utilisés CloudTrail comme type de source de données. Ces preuves contiennent les données d'origine capturées par Amazon CloudWatch, ainsi que des métadonnées supplémentaires indiquant le contrôle pris en charge par les données.
3. Audit Manager joint les éléments probants enregistrés au contrôle nommé `164.308(a)(5)(ii)(C): Administrative Safeguards - 164.308(a)(5)(ii)(C)` dans votre évaluation.

Comment utiliser Audit Manager pour démontrer la conformité à ce contrôle

Une fois les éléments probants joints au contrôle, vous (ou un délégué de votre choix) pouvez les examiner pour déterminer si des mesures correctives sont nécessaires.

Dans cet exemple, vous pouvez examiner les preuves pour voir les événements d'activation des alarmes qui ont été enregistrés par CloudTrail. Vous pouvez utiliser ce journal pour prouver que vous avez mis en place des procédures de surveillance suffisantes pour détecter les connexions à la console sans que la MFA soit activée. Si vous le souhaitez, vous pouvez également fournir des commentaires supplémentaires en ajoutant un commentaire au contrôle. Par exemple, si le journal indique plusieurs connexions sans MFA, vous pouvez ajouter un commentaire décrivant comment vous avez résolu le problème. La surveillance régulière des connexions à la console vous aide à prévenir les problèmes de sécurité pouvant découler de divergences ou de tentatives de connexion inappropriées. À son tour, cette bonne pratique contribue à mettre votre AWS environnement en conformité avec les exigences de la loi HIPAA.

Lorsque vous êtes convaincu que votre procédure de surveillance est conforme au contrôle, vous pouvez indiquer le contrôle comme étant examiné et ajouter les éléments probants à votre rapport d'évaluation. Vous pouvez ensuite partager ce rapport avec les auditeurs pour démontrer que le contrôle fonctionne comme prévu.

Contrôles manuels

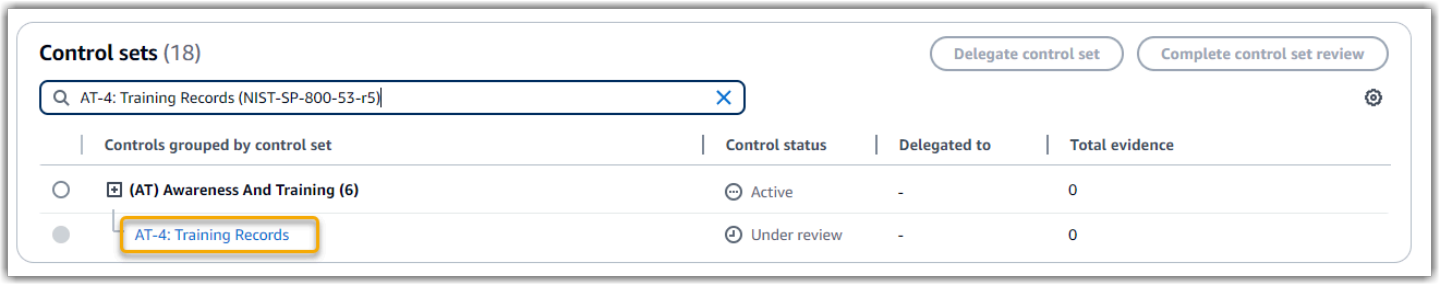
Certains contrôles ne prennent pas en charge la collecte automatisée d'éléments probants. Cela inclut les contrôles qui reposent sur la fourniture d'enregistrements physiques et de signatures, en plus des observations, des entretiens et d'autres événements qui ne sont pas générés dans le cloud. Dans ces cas, vous pouvez charger manuellement des éléments probants pour démontrer que vous répondez aux exigences du contrôle.

Cet exemple montre un contrôle manuel pour lequel Audit Manager ne recueille pas d'éléments probants automatisés. Il s'agit d'un contrôle standard issu du framework NIST 800-53 (rév. 5). Vous pouvez utiliser Audit Manager pour charger et stocker des éléments probants démontrant la conformité à ce contrôle.

Exemple de détails de contrôle

- Nom du contrôle : `AT-4: Training Records`
- Kit de commande —`(AT) Awareness and training`. Il s'agit d'un regroupement spécifique au framework de contrôles NIST liés à la formation.
- Source de preuves — Sources de données
- Type de source de données sous-jacente — Manuel
- Type d'éléments probants : manuel

Voici ce contrôle présenté dans une évaluation d'Audit Manager créée à partir du framework NIST 800-53 (rév. 5) Low-Moderate-High :



L'évaluation indique l'état du contrôle. Il montre également la quantité de preuves recueillies pour ce contrôle jusqu'à présent. À partir de là, vous pouvez déléguer l'ensemble de contrôles à des fins de révision ou l'effectuer vous-même. Le choix du nom du contrôle ouvre une page de détails contenant plus d'informations, y compris les éléments probants de ce contrôle.

Ce que réalise ce contrôle

Vous pouvez utiliser ce contrôle pour vous assurer que votre personnel reçoit le niveau approprié de formation en matière de sécurité et de confidentialité. Plus précisément, vous pouvez démontrer que vous avez mis en place des activités de formation documentées en matière de sécurité et de confidentialité pour tous les membres du personnel, en fonction de leur rôle. Vous pouvez également apporter la preuve que les dossiers de formation sont conservés pour chaque individu.

Comment charger manuellement des éléments probants pour ce contrôle

Pour télécharger des preuves manuelles qui complètent les preuves automatisées, voir Importer des preuves manuelles dans AWS Audit Manager. Audit Manager joint les éléments probants chargés au contrôle nommé `AT-4: Training Records` dans votre évaluation.

Comment utiliser Audit Manager pour démontrer la conformité à ce contrôle

Si vous disposez d'une documentation à l'appui de ce contrôle, vous pouvez la charger sous forme d'élément probant manuel. Par exemple, vous pouvez télécharger la dernière copie des supports de formation obligatoires basés sur les rôles que votre service des ressources humaines fournit aux employés.

Tout comme pour les contrôles automatisés, vous pouvez déléguer des contrôles manuels aux parties prenantes qui peuvent vous aider à examiner les éléments probants (ou, dans ce cas, à les fournir). Par exemple, lorsque vous passez en revue ce contrôle, vous constaterez peut-être que vous ne répondez que partiellement à ses exigences. Cela peut être le cas si vous n'avez aucune copie du suivi des présences pour les formations en personne. Vous pouvez déléguer le contrôle à une partie prenante des ressources humaines, qui pourra ensuite télécharger une liste des membres du personnel ayant suivi la formation.

Lorsque vous êtes convaincu que vous êtes en conformité avec le contrôle, vous pouvez l'indiquer comme étant examiné et ajouter les éléments probants à votre rapport d'évaluation. Vous pouvez ensuite partager ce rapport avec les auditeurs pour démontrer que le contrôle fonctionne comme prévu.

Contrôles utilisant des types de sources de données mixtes (automatisées et manuelles)

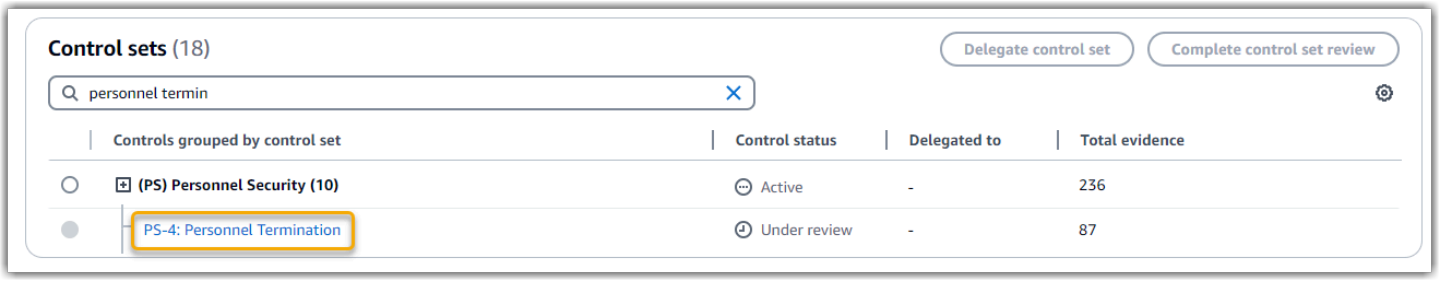
Dans de nombreux cas, il est nécessaire d'avoir une combinaison d'éléments probants automatisés et manuels pour satisfaire à un contrôle. Bien qu'Audit Manager puisse fournir des éléments probants automatisés pertinents relativement au contrôle, vous devrez peut-être compléter ces données par des éléments probants manuels que vous identifierez et chargerez vous-même.

Cet exemple montre un contrôle qui utilise une combinaison de preuves manuelles et de preuves automatisées. Il s'agit d'un contrôle standard issu du framework NIST 800-53 (rév. 5). Audit Manager utilise ce contrôle pour générer des éléments probants qui peuvent aider à mettre votre environnement AWS en conformité avec les exigences NIST.

Exemple de détails de contrôle

- Nom du contrôle : `Personnel Termination`
- Kit de commande —`(PS) Personnel Security (10)`. Il s'agit d'un regroupement de contrôles NIST spécifiques au framework qui concernent les personnes chargées de la maintenance matérielle ou logicielle des systèmes organisationnels.
- Source de preuves : sources de données AWS gérées (contrôles de base) et sources de données individuelles (manuel)
- Type de source de données sous-jacente : appels d' AWS API AWS CloudTrail,, AWS Config, manuel
- Type de preuve : données de configuration, activité de l'utilisateur, contrôle de conformité, preuves manuelles)

Voici ce contrôle présenté dans une évaluation d'Audit Manager créée à partir du framework NIST 800-53 (rév. 5) :



L'évaluation indique l'état du contrôle. Il montre également la quantité de preuves recueillies pour ce contrôle jusqu'à présent. À partir de là, vous pouvez déléguer l'ensemble de contrôles à des fins de

révision ou l'effectuer vous-même. Le choix du nom du contrôle ouvre une page de détails contenant plus d'informations, y compris les éléments probants de ce contrôle.

Ce que réalise ce contrôle

Vous pouvez utiliser ce contrôle pour confirmer que vous protégez les informations de l'organisation en cas de licenciement d'un employé. Plus précisément, vous pouvez démontrer que vous avez désactivé l'accès au système et révoqué les informations d'identification de la personne. En outre, vous pouvez démontrer que toutes les personnes licenciées ont participé à un entretien de départ qui comprenait une discussion sur les protocoles de sécurité pertinents pour votre organisation.

Fonctionnement de la collecte des éléments probants par Audit Manager pour ce contrôle

Audit Manager prend les mesures suivantes pour recueillir les éléments probants pour ce contrôle :

1. Pour chaque contrôle, Audit Manager évalue les ressources concernées à l'aide des sources de preuves spécifiées dans les paramètres de contrôle.

   Dans ce cas, le contrôle utilise plusieurs contrôles de base comme sources de preuves. À son tour, chacun de ces contrôles de base collecte des preuves pertinentes à partir de sources de données individuelles (appels d'AWS API AWS CloudTrail, et AWS Config). Audit Manager utilise ces types de sources de données pour évaluer vos ressources IAM (telles que les groupes, les clés et les politiques) par rapport aux appels d'API, aux CloudTrail événements et AWS Config aux règles pertinents.
2. Le résultat de l'évaluation des ressources est enregistré et converti en éléments probants conviviaux pour l'auditeur. Ces preuves contiennent les données d'origine capturées à partir de chaque source de données, ainsi que des métadonnées supplémentaires indiquant le contrôle pris en charge par les données.
3. Audit Manager joint les éléments probants enregistrés au contrôle nommé `Personnel Termination` dans votre évaluation.

Comment charger manuellement des éléments probants pour ce contrôle

Pour télécharger des preuves manuelles qui complètent les preuves automatisées, voir Importer des preuves manuelles dans AWS Audit Manager. Audit Manager joint les éléments probants chargés au contrôle nommé `Personnel Termination` dans votre évaluation.

Comment utiliser Audit Manager pour démontrer la conformité à ce contrôle

Une fois les éléments probants joints au contrôle, vous (ou un délégué de votre choix) pouvez les examiner pour déterminer s'ils sont suffisants ou si des mesures correctives sont nécessaires. Par exemple, lorsque vous passez en revue ce contrôle, vous constaterez peut-être que vous ne répondez que partiellement à ses exigences. Cela peut être le cas si vous avez la preuve que l'accès a été révoqué, mais que vous n'avez aucune copie des entretiens de sortie. Vous pouvez déléguer le contrôle à une partie prenante des ressources humaines, qui pourra ensuite télécharger une copie des documents relatifs à l'entretien de fin d'emploi. Ou, si aucun employé n'a été licencié pendant la période d'audit, vous pouvez laisser un commentaire expliquant pourquoi aucun document signé n'est joint au contrôle.

Lorsque vous êtes convaincu que vous êtes en conformité avec le contrôle, indiquez-le comme étant examiné et ajoutez les éléments probants à votre rapport d'évaluation. Vous pouvez ensuite partager ce rapport avec les auditeurs pour démontrer que le contrôle fonctionne comme prévu.

Intégrations avec des produits connexes Services AWS

AWS Audit Manager s'intègre Services AWS à plusieurs pour collecter automatiquement des preuves que vous pouvez inclure dans vos rapports d'évaluation.

AWS Security Hub

AWS Security Hub surveille votre environnement à l'aide de contrôles de sécurité automatisés basés sur les AWS meilleures pratiques et les normes du secteur. Audit Manager capture des instantanés du niveau de sécurité de vos ressources en signalant les résultats des contrôles de sécurité directement depuis Security Hub. Pour plus d'informations sur Security Hub, consultez Qu'est-ce que c'est AWS Security Hub ? dans le guide de AWS Security Hub l'utilisateur.

AWS CloudTrail

AWS CloudTrail vous permet de surveiller les appels effectués vers AWS les ressources de votre compte. Il s'agit notamment des appels effectués par la console de AWS gestion, la AWS CLI, Services AWS etc. Audit Manager collecte CloudTrail directement les données des journaux et convertit les journaux traités en preuves de l'activité des utilisateurs. Pour plus d'informations CloudTrail, voir Qu'est-ce que c'est AWS CloudTrail ? dans le guide de AWS CloudTrail l'utilisateur.

AWS Config

AWS Config fournit une vue détaillée de la configuration des AWS ressources de votre Compte AWS. Cela comprend des informations sur la façon dont les ressources sont interreliées et leur

configuration passée. Audit Manager capture des instantanés de votre situation en matière de sécurité des ressources en publiant les résultats directement depuis AWS Config. Pour plus d'informations AWS Config, voir Qu'est-ce que c'est AWS Config ? dans le guide de AWS Config l'utilisateur.

AWS License Manager

AWS License Manager rationalise le processus de transfert des licences des fournisseurs de logiciels vers le cloud. Au fur et à mesure que vous développez une infrastructure cloud AWS, vous pouvez réduire les coûts en réaffectant votre inventaire de licences existant pour l'utiliser avec les ressources du cloud. Audit Manager fournit un framework de gestion de licences pour vous aider à préparer votre audit. Ce framework est intégré au gestionnaire de licences pour agréger les informations d'utilisation des licences en fonction des règles de licence définies par le client. Pour plus d'informations sur License Manager, consultez Qu'est-ce que c'est AWS License Manager ? dans le guide de AWS License Manager l'utilisateur.

AWS Control Tower

AWS Control Tower met en place des garde-fous préventifs et détectifs pour l'infrastructure cloud. Audit Manager fournit un framework AWS Control Tower Guardrails pour vous aider dans la préparation de votre audit. Ce cadre contient toutes les AWS Config règles basées sur les garde-corps de. AWS Control Tower Pour plus d'informations AWS Control Tower, voir Qu'est-ce que c'est AWS Control Tower ? dans le guide de AWS Control Tower l'utilisateur.

AWS Artifact

AWS Artifact est un portail de récupération d'artefacts d'audit en libre-service qui fournit un accès à la demande à la documentation de conformité et aux certifications de l'infrastructure. AWS AWS Artifact fournit des preuves prouvant que l'infrastructure AWS cloud répond aux exigences de conformité. En revanche, il vous AWS Audit Manager aide à collecter, à examiner et à gérer les preuves pour démontrer que votre utilisation de Services AWS est conforme. Pour plus d'informations AWS Artifact, voir Qu'est-ce que c'est AWS Artifact ? dans le guide de AWS Artifact l'utilisateur. Vous pouvez télécharger la liste des AWS rapports dans le AWS Management Console.

Amazon EventBridge

Amazon vous EventBridge aide à automatiser Services AWS et à répondre automatiquement aux événements du système tels que les problèmes de disponibilité des applications ou les modifications des ressources. Vous pouvez utiliser des EventBridge règles pour détecter les événements d'Audit

Manager et y réagir. Sur la base des règles que vous créez, EventBridge invoque une ou plusieurs actions cibles lorsqu'un événement correspond aux valeurs que vous spécifiez dans une règle. En fonction du type d'événement, vous pouvez envoyer des notifications, capturer les informations sur l'événement, prendre des mesures correctives, déclencher des événements ou prendre d'autres mesures. Pour plus d'informations, consultez Surveillance AWS Audit Manager avec Amazon EventBridge.

Pour une liste des programmes Services AWS de conformité spécifiques concernés, voir Services AWS la section Portée par programme de conformité. Pour obtenir plus d'informations générales, consultez Programmes de conformitéAWS.

Intégrations avec des produits GRC tiers

AWS Audit Manager prend en charge les intégrations avec les produits GRC partenaires tiers répertoriés sur cette page.

Si votre entreprise utilise un modèle de cloud hybride ou multicloud, il est probable que vous utilisiez un produit GRC pour gérer les éléments probants issus de ces environnements. Lorsque ce produit est intégré à Audit Manager, vous pouvez extraire des preuves de votre AWS utilisation directement dans votre environnement GRC. Le faire simplifie la gestion de la conformité en vous fournissant un emplacement centralisé pour examiner et corriger les éléments probants lors de la préparation des audits.

Lisez cette page pour un aperçu des produits GRC tiers qui peuvent ingérer des éléments probants provenant d'Audit Manager. Vous pouvez également voir une référence des actions d'API d'Audit Manager que vous pouvez effectuer directement dans ces produits.

Rubriques

- Comprendre le fonctionnement des intégrations tierces avec Audit Manager
- Produits partenaires GRC tiers s'intégrant à Audit Manager

Comprendre le fonctionnement des intégrations tierces avec Audit Manager

Les partenaires GRC peuvent utiliser les API publiques d'Audit Manager pour intégrer leurs produits à Audit Manager. Une fois cette intégration en place, vous pouvez mapper les contrôles d'entreprise de votre environnement GRC aux contrôles courants fournis par Audit Manager.

> **Tip**
>
> Vous pouvez associer les contrôles de votre entreprise à n'importe quel type de contrôle Audit Manager. Toutefois, nous vous recommandons d'utiliser des commandes communes. Lorsque vous mappez un contrôle commun qui représente votre objectif, Audit Manager collecte des preuves à partir d'un groupe prédéfini de sources de données gérées par AWS. Cela signifie que vous n'avez pas besoin d'être un AWS expert pour savoir quelles sources de données collectent les preuves pertinentes pour atteindre votre objectif.

Après avoir terminé cet exercice unique de mappage des contrôles, vous pouvez créer des évaluations Audit Manager directement dans le produit GRC. Cette action lance la collecte de preuves concernant votre AWS utilisation. Vous pouvez ensuite consulter ces AWS preuves ainsi que les autres preuves collectées dans votre environnement hybride, le tout dans le même contexte que celui des contrôles de votre entreprise.

Lorsque vous utilisez une intégration Audit Manager avec un produit GRC tiers, gardez à l'esprit les points suivants :

- Les intégrations sont disponibles pour toutes les Régions AWS dans lesquelles Audit Manager est pris en charge.
- Toutes les ressources Audit Manager que vous créez dans le produit partenaire GRC sont également reflétées dans Audit Manager.
- Vous êtes soumis à une tarification AWS Audit Manager en plus de celle du produit GRC tiers.
- Les éléments probants recueillis par Audit Manager sont immuables. Les éléments probants sont présentés exactement de la même manière dans les produits GRC tiers que dans la console Audit Manager. Toutefois, si vous utilisez une intégration tierce, vous pourrez peut-être améliorer ces éléments probants en fournissant un contexte supplémentaire dans vos rapports.
- Les mêmes quotas qui s'appliquent à Audit Manager s'appliquent également au produit GRC tiers. Par exemple, chaque Compte AWS peut contenir jusqu'à 100 évaluations Audit Manager actives. Ce quota au niveau du compte s'applique, que vous créiez les évaluations dans la console Audit Manager ou dans le produit GRC tiers. La plupart des quotas d'Audit Manager, mais pas tous, sont répertoriés sous l'espace de AWS Audit Manager noms de la console Service Quotas. Pour savoir comment demander une augmentation de quota, consultez Gestion de vos quotas d'Audit Manager.

Si vous disposez d'une solution de conformité et que vous souhaitez l'intégrer à Audit Manager, envoyez un e-mail à l'adresse `auditmanager-partners@amazon.com`.

Produits partenaires GRC tiers s'intégrant à Audit Manager

Les produits GRC tiers suivants peuvent ingérer des éléments probants provenant d'Audit Manager.

MetricStream

Pour utiliser cette intégration, contactez MetricStreampour accéder au logiciel MetricStream GRC et l'acheter.

Construite sur la MetricStream plate-forme, la solution MetricStream Enterprise GRC permet une approche globale et collaborative des activités et des processus GRC à l'échelle de l'entreprise. En y intégrant les preuves provenant d'Audit Manager MetricStream, vous pouvez identifier de manière proactive les preuves non conformes provenant de votre AWS environnement et les examiner en même temps que les preuves provenant de vos sources de données sur site ou d'autres partenaires cloud. Vous disposez ainsi d'un moyen pratique et centralisé de revoir et d'améliorer votre niveau de sécurité et de conformité dans le cloud alors que vous vous préparez aux audits.

Grâce à MetricStream l'intégration avec Audit Manager, vous pouvez effectuer les opérations d'API suivantes.

Tâche	Opération API
Configuration de l'intégration d'Audit Manager	• GetAccountStatus • GetOrganizationAdminAccount • GetSettings
Examen des ressources Audit Manager	• GetAssessment • GetAssessmentFramework • GetControl • ListAssessmentFrameworks • ListControls
Créer des ressources Audit Manager	• CreateAssessment

Tâche	Opération API
	• CreateAssessmentFramework
Mettre à jour des ressources Audit Manager	• UpdateAssessment • UpdateAssessmentControl • UpdateAssessmentStatus
Gérer les éléments probants	• StartQuery(AWS CloudTrail API) • GetQueryResults(AWS CloudTrail API)
Supprimer des ressources Audit Manager	• DeleteAssessmentFramework

MetricStream Liens connexes

- AWS Marketplace lien
- Lien vers le produit
- Tarification du produit

Intégrer les preuves d'Audit Manager dans votre système GRC

En tant qu'entreprise cliente, vous disposez probablement de ressources réparties dans plusieurs centres de données, y compris d'autres fournisseurs de cloud et dans des environnements sur site. Pour collecter des preuves à partir de ces environnements, vous pouvez utiliser des solutions GRC (gouvernance, risque et conformité) tierces telles que MetricStream CyberGRC ou RSA Archer. Vous pouvez également utiliser un système GRC propriétaire que vous avez développé en interne.

Ce tutoriel explique comment intégrer votre système GRC interne ou externe à Audit Manager. Cette intégration permet aux fournisseurs de collecter des preuves concernant AWS l'utilisation et les configurations de leurs clients, et de les envoyer directement depuis Audit Manager vers l'application GRC. Vous pouvez ainsi centraliser vos rapports de conformité dans plusieurs environnements.

Dans le cadre de ce didacticiel :

1. Un fournisseur est l'entité ou l'entreprise propriétaire de l'application GRC intégrée à Audit Manager.

2. Un client est l'entité ou l'entreprise qui utilise AWS, et qui utilise également une application GRC interne ou externe.

> **Note**
>
> Dans certains cas, l'application GRC est détenue et utilisée par la même entreprise. Dans ce scénario, le fournisseur est le groupe ou l'équipe propriétaire de l'application GRC, et le client est l'équipe ou le groupe qui utilise l'application GRC.

Ce didacticiel vous montre comment effectuer les opérations suivantes :

- Étape 1 : activer Audit Manager
- Étape 2 : configurer les autorisations
- Étape 3. Associez les contrôles de votre entreprise aux contrôles d'Audit Manager
- Étape 4 : Maintenez vos mappages de contrôle à jour
- Étape 5 : Création d'une évaluation
- Étape 6. Commencez à recueillir des preuves

Prérequis

Avant de commencer, assurez-vous de remplir les conditions suivantes :

- Vous disposez d'une infrastructure en cours d'exécution AWS.
- Vous utilisez un système GRC interne ou un logiciel GRC tiers fourni par un fournisseur.
- Vous avez rempli toutes les conditions requises pour configurer Audit Manager.
- Tu connais bienComprendre AWS Audit Manager les concepts et la terminologie.

Quelques restrictions à garder à l'esprit :

- L'Audit Manager est un responsable régional Service AWS. Vous devez configurer Audit Manager séparément dans chaque région dans laquelle vous exécutez vos AWS charges de travail.
- Audit Manager ne prend pas en charge l'agrégation de preuves provenant de plusieurs régions au sein d'une seule région. Si vos ressources sont multiples Régions AWS, vous devez agréger les preuves au sein de votre système GRC.

- Audit Manager dispose de quotas par défaut pour le nombre de ressources que vous pouvez créer. Vous pouvez demander une augmentation de ces quotas par défaut si nécessaire. Pour plus d'informations, consultez la section Quotas et restrictions pour AWS Audit Manager.

Étape 1 : activer Audit Manager

Qui complète cette étape

Client

Ce que vous devez faire

Commencez par activer Audit Manager pour votre Compte AWS. Si votre compte fait partie d'une organisation, vous pouvez activer Audit Manager à l'aide de votre compte de gestion, puis spécifier un administrateur délégué pour Audit Manager.

Procédure

Pour activer Audit Manager

Suivez les instructions pour activer Audit Manager. Répétez la procédure de configuration pour toutes les régions dans lesquelles vous souhaitez collecter des preuves.

> **Tip**
>
> Si vous l'utilisez AWS Organizations, nous vous recommandons vivement de configurer un administrateur délégué au cours de cette étape. Lorsque vous utilisez un compte d'administrateur délégué dans Audit Manager, vous pouvez utiliser l'outil de recherche de preuves pour rechercher des preuves sur tous les comptes membres de votre organisation.

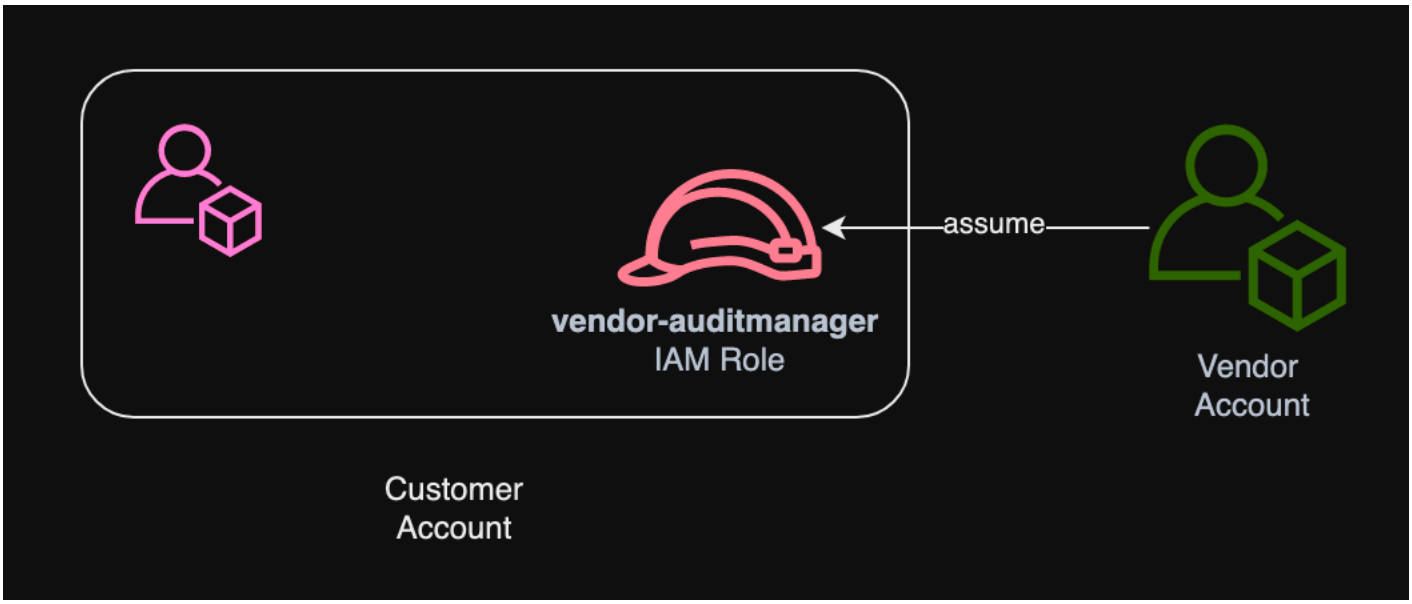
Étape 2 : configurer les autorisations

Qui complète cette étape

Client

Ce que vous devez faire

Au cours de cette étape, le client crée un rôle IAM pour son compte. Le client donne ensuite au fournisseur l'autorisation d'assumer le rôle.



Procédure

Pour créer un rôle pour le compte client

Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM du Guide de l'utilisateur IAM.

- À l'étape 8 du flux de travail de création de rôle, choisissez Créer une politique et entrez une politique pour le rôle.

  Le rôle doit au minimum disposer des autorisations suivantes :

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AuditManagerAccess",
      "Effect" : "Allow",
      "Action" : [
        "auditmanager:*"
      ],
      "Resource" : "*"
    },
```

```
    {
      "Sid" : "OrganizationsAccess",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAccountsForParent",
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListChildren"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "IAMAccess",
      "Effect" : "Allow",
      "Action" : [
        "iam:GetUser",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "S3Access",
      "Effect" : "Allow",
      "Action" : [
        "s3:ListAllMyBuckets"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsAccess",
      "Effect" : "Allow",
      "Action" : [
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "KmsCreateGrantAccess",
```

```
      "Effect" : "Allow",
      "Action" : [
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        },
        "StringLike" : {
          "kms:ViaService" : "auditmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "SNSAccess",
      "Effect" : "Allow",
      "Action" : [
        "sns:ListTopics"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "TagAccess",
      "Effect" : "Allow",
      "Action" : [
        "tag:GetResources"
      ],
      "Resource" : "*"
    }
  ]
}
```

- À l'étape 11 du flux de travail de création de rôles, entrez le `vendor-auditmanager` nom du rôle.

Pour autoriser le compte fournisseur à assumer le rôle

Suivez les instructions de la section Accorder aux utilisateurs l'autorisation de changer de rôle dans le Guide de l'utilisateur IAM.

- La déclaration de politique doit inclure l'`Allow`effet sur le`sts:AssumeRole action`.
- Il doit également inclure l'Amazon Resource Name (ARN) du rôle dans un élément Resource.

- Voici un exemple de déclaration de politique que vous pouvez utiliser.

  Dans cette politique, remplacez le *texte de l'espace réservé* par l' Compte AWS identifiant de votre fournisseur.

```
{
 "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::account-id:role/vendor-auditmanager"
  }
}
```

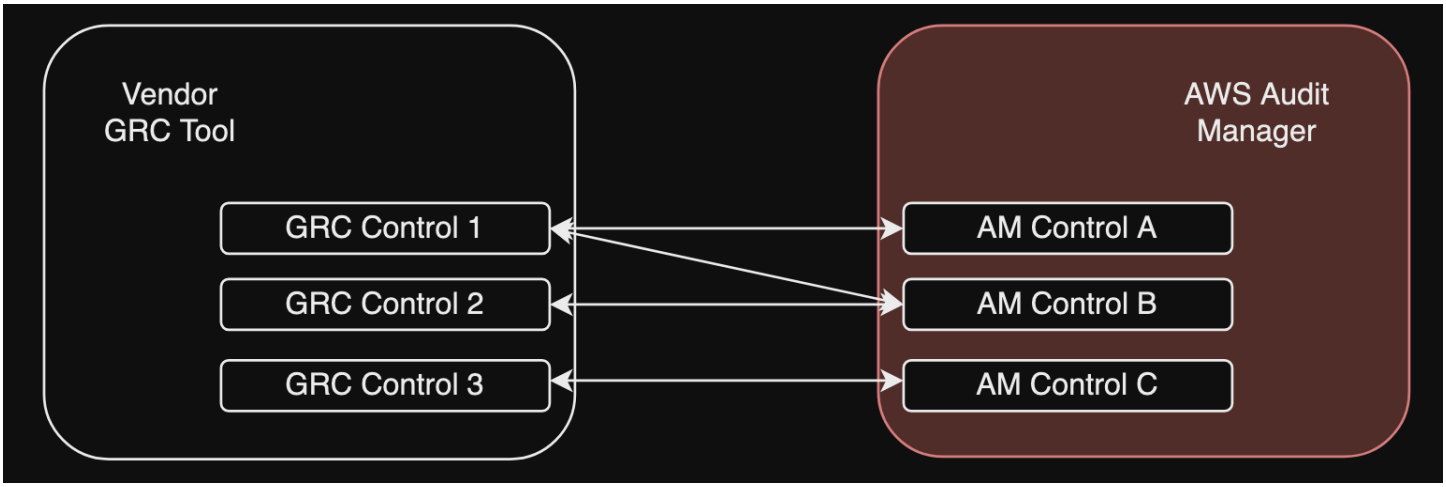
Étape 3. Associez les contrôles de votre entreprise aux contrôles d'Audit Manager

Qui complète cette étape

Client

Ce que vous devez faire

Les fournisseurs tiennent à jour une liste organisée des contrôles d'entreprise que les clients peuvent utiliser dans le cadre d'une évaluation. Pour intégrer Audit Manager, les fournisseurs doivent créer une interface permettant aux clients de mapper les contrôles de leur entreprise aux contrôles d'Audit Manager correspondants. Vous pouvez mapper vers common control s (préféré) ou standard control s. Vous devez terminer ce mappage avant de commencer toute évaluation dans l'application GRC du fournisseur.



Option 1 : associer les contrôles d'entreprise aux contrôles communs (recommandé)

Il s'agit de la méthode recommandée pour mapper les contrôles de votre entreprise à Audit Manager. Cela s'explique par le fait que les contrôles communs sont étroitement liés aux normes industrielles communes. Il est ainsi plus facile de les associer aux contrôles de votre entreprise.

Avec cette approche, le fournisseur crée une interface qui permet au client d'effectuer un mappage ponctuel entre ses contrôles d'entreprise et les contrôles communs correspondants fournis par Audit Manager. Les fournisseurs peuvent utiliser les opérations ListControlsListCommonControls,, et GetControlAPI pour communiquer ces informations aux clients. Une fois que le client a terminé l'exercice de mappage, le fournisseur peut utiliser ces mappages pour créer des contrôles personnalisés dans Audit Manager.

Voici un exemple de mappage de contrôle courant :

Supposons que vous ayez nommé un contrôle d'entrepriseAsset Management. Ce contrôle d'entreprise correspond à deux contrôles courants dans Audit Manager (Asset performance managementetAsset maintenance scheduling). Dans ce cas, vous devez créer un contrôle personnalisé dans Audit Manager (nous allons le nommerenterprise-asset-management). Ensuite, ajoutez Asset performance management et Asset maintenance scheduling en tant que sources de preuves au nouveau contrôle personnalisé. Ces sources de preuves collectent des preuves à l'appui à partir d'un groupe prédéfini de sources de AWS données. Vous disposez ainsi d'un moyen efficace d'identifier les sources de AWS données correspondant aux exigences du contrôle de votre entreprise.

Procédure

Pour trouver les commandes communes disponibles auxquelles vous pouvez mapper

Suivez les étapes pour trouver la liste des contrôles courants disponibles dans Audit Manager.

Pour créer un contrôle personnalisé

1. Suivez les étapes pour créer un contrôle personnalisé qui s'aligne sur le contrôle de votre entreprise.

   Lorsque vous spécifiez des sources de preuves à l'étape 2 du flux de travail de création de contrôles personnalisés, procédez comme suit :

   - Choisissez des sources AWS gérées comme source de preuves.
   - Sélectionnez Utiliser un contrôle commun correspondant à votre objectif de conformité.
   - Choisissez jusqu'à cinq contrôles courants comme sources de preuves pour le contrôle de votre entreprise.
2. Répétez cette tâche pour tous les contrôles de votre entreprise et créez les contrôles personnalisés correspondants dans Audit Manager pour chacun d'entre eux.

Option 2 : associer les contrôles d'entreprise aux contrôles standard

Audit Manager fournit un grand nombre de contrôles standard prédéfinis. Vous pouvez effectuer un mappage ponctuel entre les contrôles de votre entreprise et ces contrôles standard. Une fois que vous avez identifié les contrôles standard correspondant aux contrôles de votre entreprise, vous pouvez les ajouter directement à un cadre personnalisé. Si vous choisissez cette option, vous n'avez pas besoin de créer de contrôles personnalisés dans Audit Manager.

Procédure

Pour trouver les commandes standard disponibles auxquelles vous pouvez mapper

Suivez les étapes pour trouver la liste des contrôles standard disponibles dans Audit Manager.

Pour créer un cadre personnalisé

1. Suivez les étapes pour créer un framework personnalisé dans Audit Manager.

   Lorsque vous spécifiez un ensemble de contrôles à l'étape 2 de la procédure de création du framework, incluez les contrôles standard qui correspondent aux contrôles de votre entreprise.
2. Répétez cette tâche pour tous les contrôles de votre entreprise jusqu'à ce que vous ayez inclus tous les contrôles standard correspondants dans votre cadre personnalisé.

Étape 4 : Maintenez vos mappages de contrôle à jour

Qui complète cette étape

Vendeur, client

Ce que vous devez faire

Audit Manager met à jour en permanence les contrôles courants et les contrôles standard pour s'assurer qu'ils utilisent les dernières sources de AWS données disponibles. Cela signifie que le mappage des contrôles est une tâche ponctuelle : vous n'avez pas besoin de gérer les contrôles standard après les avoir ajoutés à un cadre personnalisé, et vous n'avez pas besoin de gérer les contrôles communs une fois que vous les avez ajoutés en tant que source de preuves dans votre contrôle personnalisé. Chaque fois qu'un contrôle commun est mis à jour, les mêmes mises à jour sont automatiquement appliquées à tous les contrôles personnalisés qui utilisent ce contrôle commun comme source de preuves.

Cependant, au fil du temps, il est possible que de nouveaux contrôles communs et standards soient disponibles pour que vous puissiez les utiliser comme sources de preuves. Dans cette optique, les fournisseurs et les clients doivent créer un flux de travail pour récupérer régulièrement les derniers contrôles courants et les contrôles standard auprès d'Audit Manager. Vous pouvez ensuite passer en revue les mappages entre les contrôles d'entreprise et les contrôles Audit Manager, et mettre à jour les mappages selon vos besoins.

Si les contrôles de votre entreprise sont mappés à des contrôles communs

Au cours du processus de mappage, vous avez créé des contrôles personnalisés. Vous pouvez utiliser Audit Manager pour modifier ces contrôles personnalisés afin qu'ils utilisent les derniers contrôles courants disponibles comme sources de preuves. Une fois les mises à jour des contrôles personnalisés entrées en vigueur, vos évaluations existantes collecteront automatiquement des preuves par rapport aux contrôles personnalisés mis à jour. Il n'est pas nécessaire de créer un nouveau cadre ou une nouvelle évaluation.

Procédure

Pour trouver les derniers contrôles courants auxquels vous pouvez mapper

Suivez les étapes pour trouver les contrôles courants disponibles dans Audit Manager.

Pour modifier un contrôle personnalisé

1. Suivez les étapes pour modifier un contrôle personnalisé dans Audit Manager.

   Lorsque vous mettez à jour les sources de preuves à l'étape 2 du processus de modification, procédez comme suit :

   - Choisissez des sources AWS gérées comme source de preuves.
   - Sélectionnez Utiliser un contrôle commun correspondant à votre objectif de conformité.
   - Choisissez le nouveau contrôle commun que vous souhaitez utiliser comme source de preuves pour votre contrôle personnalisé.
2. Répétez cette tâche pour tous les contrôles d'entreprise que vous souhaitez mettre à jour.

Si les contrôles de votre entreprise sont mappés aux contrôles standard

Dans ce cas, les fournisseurs doivent créer un nouveau cadre personnalisé qui inclut les derniers contrôles standard disponibles, puis créer une nouvelle évaluation à l'aide de ce nouveau cadre. Après avoir créé la nouvelle évaluation, vous pouvez marquer votre ancienne évaluation comme inactive.

Procédure

Pour trouver les dernières commandes standard auxquelles vous pouvez mapper

Suivez les étapes pour trouver les contrôles standard disponibles dans Audit Manager.

Pour créer un cadre personnalisé et ajouter les derniers contrôles standard

Suivez les étapes pour créer un framework personnalisé dans Audit Manager.

Lorsque vous spécifiez un ensemble de contrôles à l'étape 2 du flux de travail de création du framework, incluez les nouveaux contrôles standard.

Pour créer une évaluation

Créez une évaluation dans l'application GRC.

Pour faire passer le statut d'une évaluation à inactif

Suivez les étapes pour modifier le statut d'une évaluation dans Audit Manager.

Étape 5 : Création d'une évaluation

Qui complète cette étape

Application GRC, avec contribution du fournisseur

Ce que vous devez faire

En tant que client, vous n'avez pas besoin de créer une évaluation directement dans Audit Manager. Lorsque vous lancez une évaluation pour certains contrôles dans l'application GRC, l'application GRC crée les ressources correspondantes pour vous dans Audit Manager. Tout d'abord, l'application GRC utilise les mappages que vous avez créés pour identifier les contrôles Audit Manager pertinents. Ensuite, il utilise les informations de contrôle pour créer un cadre personnalisé pour vous. Enfin, il utilise le nouveau framework personnalisé pour créer une évaluation dans Audit Manager.

La création d'une évaluation dans Audit Manager nécessite également un champ d'application. Ce champ d'application prend une liste des Comptes AWS endroits où le client souhaite effectuer l'évaluation et recueillir des preuves. Les clients doivent définir cette étendue directement dans l'application GRC.

En tant que fournisseur, vous devez stocker le `assessmentId` mappé à l'évaluation lancée dans l'application GRC. Cela `assessmentId` est nécessaire pour récupérer des preuves auprès d'Audit Manager.

Pour trouver un identifiant d'évaluation

1. Utilisez cette ListAssessmentsopération pour afficher vos évaluations dans Audit Manager. Vous pouvez utiliser le paramètre d'état pour afficher les évaluations actives.

   ```
   aws auditmanager list-assessments --status ACTIVE
   ```

2. Dans la réponse, identifiez l'évaluation que vous souhaitez stocker dans l'application GRC et prenez note du`assessmentId`.

Étape 6. Commencez à recueillir des preuves

Qui complète cette étape

AWS Audit Manager, avec la contribution du fournisseur

Ce que vous devez faire

Une fois que vous avez créé une évaluation, il faut jusqu'à 24 heures pour commencer à recueillir des preuves. À ce stade, les contrôles de votre entreprise collectent désormais activement des preuves pour votre évaluation d'Audit Manager.

Nous vous recommandons d'utiliser la fonction de recherche de preuves pour rechercher et trouver rapidement des preuves dans Audit Manager. Si vous utilisez la recherche d'éléments probants en tant qu'administrateur délégué, vous pouvez inclure tous les comptes membres de votre organisation dans votre recherche. Vous pouvez affiner votre requête de recherche à l'aide de filtres et de regroupements. Par exemple, si vous souhaitez obtenir une vue d'ensemble de l'état de votre système, effectuez une recherche approfondie et filtrez par évaluation, plage de dates et conformité des ressources. Si votre objectif est de remédier à une ressource spécifique, vous pouvez effectuer une recherche précise afin de cibler les éléments probants d'un contrôle ou d'un identifiant de ressource spécifique. Après avoir défini vos filtres, vous pouvez regrouper puis prévisualiser les résultats de recherche correspondants, avant de créer un rapport d'évaluation.

Pour activer l'outil de recherche de preuves

- Suivez les instructions pour activer l'outil de recherche de preuves dans les paramètres de l'Audit Manager.

Après avoir activé l'outil de recherche de preuves, vous pouvez choisir une cadence pour récupérer les preuves auprès d'Audit Manager pour votre évaluation. Vous pouvez également récupérer les preuves d'un contrôle spécifique dans le cadre d'une évaluation et les stocker dans l'application GRC mappée au contrôle d'entreprise. Vous pouvez utiliser les opérations d'API Audit Manager suivantes pour récupérer des preuves :

- GetEvidence
- GetEvidenceByEvidenceFolder
- GetEvidenceFolder
- GetEvidenceFoldersByAssessment
- GetEvidenceFoldersByAssessmentControl

Tarification

Cette configuration d'intégration ne vous coûtera aucun coût supplémentaire, que vous soyez fournisseur ou client. Les clients sont facturés pour les preuves collectées dans Audit Manager. Pour plus d'informations sur la tarification, consultez Tarification d'AWS Audit Manager.

Ressources supplémentaires

Pour en savoir plus sur les concepts présentés dans ce didacticiel, consultez les ressources suivantes :

- Évaluations : découvrez les concepts et les tâches liés à la gestion d'une évaluation.
- Bibliothèque de contrôles : découvrez les concepts et les tâches de gestion d'un contrôle personnalisé.
- Bibliothèque de cadres : découvrez les concepts et les tâches de gestion d'un framework personnalisé.
- Outil de recherche de preuves : découvrez comment exporter un fichier CSV ou générer un rapport d'évaluation à partir des résultats de vos requêtes.
- Centre de téléchargement - Découvrez comment télécharger des rapports d'évaluation et des exportations CSV depuis Audit Manager.

Frameworks pris en charge dans AWS Audit Manager

Lorsque vous explorez la bibliothèque de frameworks dans AWS Audit Manager, vous trouverez une liste complète de frameworks standard prédéfinis qui peuvent vous aider à rationaliser vos efforts de mise en conformité. Ces frameworks prédéfinis sont basés sur les AWS meilleures pratiques relatives à diverses normes et réglementations de conformité. Vous pouvez utiliser ces cadres pour vous aider à préparer votre audit, que vous ayez besoin d'évaluer votre environnement par rapport aux normes HIPAA, PCI DSS, SOC 2 ou à d'autres normes.

La liste suivante fournit un aperçu des frameworks disponibles afin que vous puissiez facilement identifier ceux qui correspondent à vos besoins spécifiques. Prenez le temps de consulter la liste et de vous familiariser avec les cadres les plus adaptés aux besoins de votre organisation. Ouvrez n'importe quelle page pour avoir une vue d'ensemble de ce cadre et découvrir comment vous pouvez l'utiliser pour créer une évaluation et commencer à collecter des preuves dans Audit Manager.

Rubriques

- GDPR 2016
- Loi Gramm-Leach-Bliley
- Titre 21 CFR Part 11
- Annexe 11 des normes GMP de l'UE, v1
- Règle de sécurité HIPAA : février 2003
- Règle finale omnibus HIPAA
- ISO/IEC 27001:2013 Annexe A
- NIST SP 800-53 Rév. 5
- Cadre de cybersécurité du NIST v1.1
- NIST SP 800-171 Rév. 2
- PCI DSS V3.2.1
- PCI DSS V4.0
- ÉSAE-18 SOC 2

ACSC Essential Eight

AWS Audit Manager fournit un cadre standard prédéfini qui prend en charge l'Australian Cyber Security Center (ACSC) Essential Eight.

Rubriques

- Qu'est-ce que l'ACSC Essential Eight ?
- Utilisation de ce framework
- Étapes suivantes
- Ressources supplémentaires

Qu'est-ce que l'ACSC Essential Eight ?

L'ACSC est l'agence principale du gouvernement australien en matière de cybersécurité. Pour se protéger contre les cybermenaces, l'ACSC recommande aux organisations de mettre en œuvre huit stratégies d'atténuation essentielles issues des Stratégies d'atténuation des incidents de cybersécurité de l'ACSC comme base de référence. Cette base de référence, connue sous le nom d'Essential Eight, rend beaucoup plus difficile pour les adversaires de compromettre les systèmes.

Comme l'Essential Eight décrit un ensemble minimal de mesures préventives, votre organisation doit mettre en œuvre des mesures supplémentaires lorsque cela est justifié par votre environnement. En outre, bien que l'Essential Eight puisse aider à atténuer la majorité des cybermenaces, il n'atténuera pas toutes les cybermenaces. À ce titre, des stratégies d'atténuation et des contrôles de sécurité supplémentaires doivent être envisagés, notamment ceux figurant dans les Stratégies d'atténuation des incidents de cybersécurité et le Manuel de sécurité de l'information (ISM).

Utilisation de ce framework

Vous pouvez utiliser le cadre standard Essential Eight AWS Audit Manager pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences d'Essential Eight. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le framework Essential Eight. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Centre australien de cybersécurité (ACSC) Essential Eight	144	49	3

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _ASCS-Essential-Eight.zip.

Les contrôles de ce AWS Audit Manager cadre ne sont pas destinés à vérifier si vos systèmes sont conformes aux contrôles Essential Eight. De plus, ils ne peuvent garantir que vous passerez un audit ACSC. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous trouverez le framework Essential Eight sous l'onglet Cadres standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- ACSC Essential Eight

ACSC ISM 02 mars 2023

AWS Audit Manager fournit un cadre standard prédéfini qui prend en charge le manuel de sécurité de l'information (ISM) du Centre australien de cybersécurité (ACSC).

Rubriques

- Qu'est-ce que l'ACSC ISM ?
- Utilisation de ce framework

- Étapes suivantes
- Ressources supplémentaires

Qu'est-ce que l'ACSC ISM ?

L'ACSC est l'agence principale du gouvernement australien en matière de cybersécurité. L'ACSC produit l'ISM, qui fonctionne comme un ensemble de principes de cybersécurité. L'objectif de ces principes est de fournir des conseils stratégiques sur la manière dont une organisation peut protéger ses systèmes et ses données des cybermenaces. Ces principes de cybersécurité sont regroupés en quatre activités principales : gouverner, protéger, détecter et intervenir. Une organisation doit être en mesure de démontrer que les principes de cybersécurité sont respectés au sein de son organisation. L'ISM est destiné aux responsables de la sécurité de l'information, aux directeurs des systèmes d'information, aux professionnels de la cybersécurité et aux responsables des technologies de l'information.

Utilisation de ce framework

Vous pouvez utiliser le cadre standard ACSC ISM pour vous aider AWS Audit Manager à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces commandes sont regroupées en ensembles de commandes conformément aux exigences ACSC ISM. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le cadre ACSC ISM. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Manuel de sécurité de l'information (ISM) du Centre australien de cybersécurité (ACSC) 02 mars 2023	557	320	22

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _ACSC-ISM-02-March-2023.zip.

Les contrôles de ce AWS Audit Manager cadre ne sont pas destinés à vérifier si vos systèmes sont conformes aux contrôles du manuel de sécurité de l'information de l'ACSC. De plus, ils ne peuvent garantir que vous passerez un audit ACSC. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous pouvez trouver le framework ACSC ISM sous l'onglet Cadres standard de la bibliothèque de cadres dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- Manuel de sécurité de l'information ACSC

AWS Audit Manager Exemple de cadre

AWS Audit Manager fournit un exemple de cadre prédéfini pour vous aider à démarrer la préparation de votre audit.

Rubriques

Qu'est-ce que l' AWS Audit Manager exemple de framework ?

Le AWS Audit Manager Sample Framework est un framework simple que vous pouvez utiliser pour démarrer dans Audit Manager. Certains des autres frameworks prédéfinis fournis par Audit Manager sont en comparaison beaucoup plus volumineux et contiennent de nombreux contrôles. En utilisant le framework type au lieu de ces frameworks plus volumineux, vous pouvez examiner et explorer plus facilement un exemple de framework. Les contrôles de ce framework sont basés sur une série de AWS Config règles et d'appels AWS d'API.

Utilisation de ce framework

Vous pouvez utiliser ce framework pour vous aider à démarrer dans Audit Manager. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le AWS Audit Manager Sample Framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des preuves pertinentes pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le framework. Ensuite, il recueille les éléments probants pertinents, puis les associe aux contrôles de votre évaluation.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Exemple de framework d'Audit Manager pour Amazon Web Services (AWS)	5	0	3

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _AWS-Audit-Manager-Sample-Framework.zip.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

AWS Control Tower Rambardes

AWS Audit Manager fournit un framework AWS Control Tower Guardrails prédéfini pour vous aider dans la préparation de votre audit.

Rubriques

- Qu'est-ce que c'est AWS Control Tower ?
- Utilisation de ce framework

- Étapes suivantes
- Ressources supplémentaires

Qu'est-ce que c'est AWS Control Tower ?

AWS Control Tower est un service de gestion et de gouvernance que vous pouvez utiliser pour parcourir le processus de configuration et les exigences de gouvernance nécessaires à la création d'un AWS environnement multi-comptes.

Avec AWS Control Tower, vous pouvez en fournir de nouvelles Comptes AWS conformes aux politiques de votre entreprise ou de votre organisation en quelques clics. AWS Control Tower crée une couche d'orchestration en votre nom qui combine et intègre les capacités de plusieurs autres Services AWS. Ces services incluent AWS Organizations AWS IAM Identity Center, et Service AWS Catalog. Cela permet de simplifier le processus de configuration et de gouvernance de l'environnement AWS multi-comptes, de façon sécurisée et conforme.

Le framework AWS Control Tower Guardrails contient tous ceux AWS Config Rules qui sont basés sur des rambardes de. AWS Control Tower

Utilisation de ce framework

Vous pouvez utiliser le framework de barrières de protection AWS Control Tower pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces commandes sont regroupées en fonction de celles basées sur AWS Config Rules les rambardes de sécurité de. AWS Control Tower Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des preuves pertinentes pour un AWS Control Tower audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le framework AWS Control Tower Guardrails. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework AWS Control Tower Guardrails sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
AWS Control Tower Rambardes	14	0	5

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _AWS-Control-Tower-Guardrails.zip.

Les contrôles de ce AWS Audit Manager cadre ne sont pas destinés à vérifier si vos systèmes sont conformes à AWS Control Tower Guardrails. De plus, ils ne peuvent pas garantir que vous passerez un audit.

Vous trouverez le framework AWS Control Tower Guardrails sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- AWS Control Tower page de service
- AWS Control Tower guide de l'utilisateur

AWS cadre des meilleures pratiques d'IA générative v2

> **Note**
>
> Le 11 juin 2024, j'ai AWS Audit Manager mis à niveau ce framework vers une nouvelle version, le framework des meilleures pratiques d'IA AWS générative v2. En plus de soutenir les meilleures pratiques pour Amazon Bedrock, la version v2 vous permet de recueillir des preuves démontrant que vous suivez les meilleures pratiques sur Amazon SageMaker.
> Le framework de bonnes pratiques d'IA AWS générative v1 n'est plus pris en charge. Si vous avez déjà créé une évaluation à partir du framework v1, vos évaluations existantes continueront de fonctionner. Cependant, vous ne pouvez plus créer de nouvelles évaluations à partir du framework v1. Nous vous encourageons à utiliser plutôt le framework mis à jour vers la version v2.

AWS Audit Manager fournit un cadre standard prédéfini pour vous aider à mieux comprendre comment votre mise en œuvre de l'IA générative sur Amazon Bedrock et Amazon SageMaker fonctionne par rapport aux meilleures pratiques AWS recommandées.

Amazon Bedrock est un service entièrement géré qui met à disposition des modèles d'IA d'Amazon et d'autres grandes entreprises d'IA via une API. Avec Amazon Bedrock, vous pouvez ajuster en privé les modèles existants avec les données de votre organisation. Cela vous permet d'exploiter les modèles de fondation (FM) et les grands modèles de langage (LLM) pour créer des applications en toute sécurité, sans compromettre la confidentialité des données. Pour de plus amples informations, veuillez consulter Qu'est-ce qu'Amazon Bedrock ? dans le Guide de l'utilisateur Amazon Bedrock.

Amazon SageMaker est un service d'apprentissage automatique (ML) entièrement géré. Les data scientists et les développeurs peuvent ainsi créer, former et déployer des modèles de machine learning pour des cas d'utilisation étendus qui nécessitent une personnalisation approfondie et un ajustement précis des modèles. SageMaker SageMaker fournit des algorithmes de machine learning gérés pour fonctionner efficacement sur des données extrêmement volumineuses dans un environnement distribué. Grâce à la prise en charge intégrée de vos propres algorithmes et frameworks, il SageMaker propose des options de formation distribuées flexibles qui s'adaptent à vos flux de travail spécifiques. Pour plus d'informations, consultez Qu'est-ce qu'Amazon SageMaker ? dans le guide de SageMaker l'utilisateur Amazon.

Rubriques

Quelles sont les meilleures pratiques en matière d'IA AWS générative pour Amazon Bedrock ?

L'IA générative fait référence à une branche de l'IA qui vise à permettre aux machines de générer du contenu. Les modèles d'IA générative sont conçus pour créer des résultats qui ressemblent étroitement aux exemples sur lesquels ils ont été formés. Cela crée des scénarios dans lesquels l'IA peut imiter la conversation humaine, générer du contenu créatif, analyser de vastes volumes de données et automatiser des processus normalement effectués par des humains. La croissance rapide de l'IA générative apporte de nouvelles innovations prometteuses. Dans le même temps, cela soulève de nouveaux défis quant à la manière d'utiliser l'IA générative de manière responsable et conformément aux exigences de gouvernance.

AWS s'engage à vous fournir les outils et les conseils nécessaires pour créer et gérer des applications de manière responsable. Pour vous aider à atteindre cet objectif, Audit Manager s'est associé à Amazon Bedrock SageMaker afin de créer le framework de bonnes pratiques en matière d'IA AWS générative v2. Ce framework vous fournit un outil spécialement conçu pour surveiller et améliorer la gouvernance de vos projets d'IA générative sur Amazon Bedrock et Amazon. SageMaker Vous pouvez utiliser les bonnes pratiques de ce framework pour renforcer le contrôle et la visibilité de l'utilisation de votre modèle et rester informé du comportement de celui-ci.

Les contrôles de ce cadre ont été développés en collaboration avec des experts en IA, des praticiens de la conformité, des spécialistes de l'assurance sécurité de tous horizons AWS, et avec la contribution de Deloitte. Chaque contrôle automatisé correspond à une source de AWS données à partir de laquelle Audit Manager collecte des preuves. Vous pouvez utiliser les éléments probants recueillis pour évaluer votre mise en œuvre de l'IA générative sur la base des huit principes suivants :

1. Responsable : Élaborer et respecter des directives éthiques pour le déploiement et l'utilisation de modèles d'IA générative
2. Sûr : Établir des paramètres clairs et des limites éthiques pour empêcher la production de résultats nocifs ou problématiques

3. Équitable : Considérer et respecter l'impact d'un système d'IA sur les différentes sous-populations d'utilisateurs
4. Durable : Viser une plus grande efficacité et des sources d'énergie plus durables
5. Résilience : Maintenir les mécanismes d'intégrité et de disponibilité pour garantir le fonctionnement fiable d'un système d'IA
6. Confidentialité : S'assurer que les données sensibles sont protégées contre le vol et la divulgation
7. Précision : Créer des systèmes d'IA précis, fiables et robustes
8. Sécurisé : Empêcher l'accès non autorisé aux systèmes d'IA générative

Exemple

Supposons que votre application utilise un modèle de fondation tiers disponible sur Amazon Bedrock. Vous pouvez utiliser le cadre des meilleures pratiques d'IA AWS générative pour surveiller votre utilisation de ce modèle. En utilisant ce framework, vous pouvez collecter des éléments probants démontrant que votre utilisation est conforme aux bonnes pratiques en matière d'IA générative. Cela vous fournit une approche cohérente pour tracer l'utilisation du modèle de suivi et les autorisations, signaler les données sensibles et être alerté en cas de divulgation involontaire. Par exemple, les contrôles spécifiques de ce framework peuvent collecter des éléments probants qui vous aident à démontrer que vous avez mis en œuvre des mécanismes pour les éléments suivants :

- Documenter la source, la nature, la qualité et le traitement des nouvelles données, afin de garantir la transparence et de faciliter la résolution de problèmes ou les audits (Responsable)
- Évaluer régulièrement le modèle à l'aide de mesures de performance prédéfinies pour garantir qu'il répond aux normes de précision et de sécurité (Sûr)
- Utiliser des outils de surveillance automatisés pour détecter et signaler les résultats ou comportements potentiellement biaisés en temps réel (Équitable)
- Évaluer, identifier et documenter l'utilisation des modèles et des scénarios dans lesquels les modèles existants peuvent être réutilisés, que vous les ayez générés ou non (Durable)
- Mettre en place des procédures de notification en cas de fuite accidentelle d'informations personnelles ou de divulgation involontaire (Confidentialité)
- Mettre en place une surveillance en temps réel du système d'IA et des alertes en cas d'anomalie ou de perturbation (Résilience)
- Détecter les inexactitudes et effectuer une analyse approfondie des erreurs pour en comprendre les causes profondes (Précision)

- Mise en œuvre du end-to-end chiffrement des données d'entrée et de sortie des modèles d'IA conformément aux normes minimales de l'industrie (sécurisé)

Utiliser ce framework pour faciliter la préparation de votre audit

> **Note**
>
> - Si vous êtes un SageMaker client ou un client d'Amazon Bedrock, vous pouvez utiliser ce framework directement dans Audit Manager. Assurez-vous d'utiliser le framework et d'effectuer des évaluations dans les Comptes AWS et régions dans lesquels vous exécutez vos modèles et applications d'IA générative.
> - Si vous souhaitez chiffrer vos CloudWatch journaux pour Amazon Bedrock ou SageMaker avec votre propre clé KMS, assurez-vous qu'Audit Manager a accès à cette clé. Pour ce faire, vous pouvez choisir votre clé gérée par le client dans les Configuration de vos paramètres de chiffrement des données paramètres de l'Audit Manager.
> - Ce framework utilise l'ListCustomModelsopération Amazon Bedrock pour générer des preuves concernant l'utilisation de votre modèle personnalisé. Cette opération d'API est actuellement prise en charge Régions AWS uniquement dans l'est des États-Unis (Virginie du Nord) et dans l'ouest des États-Unis (Oregon). Pour cette raison, il est possible que vous n'ayez accès à aucun élément probant concernant l'utilisation de vos modèles personnalisés dans les régions Asie-Pacifique (Tokyo), Asie Pacifique (Singapour) ou Europe (Francfort).

Vous pouvez utiliser ce framework pour vous aider à préparer les audits concernant votre utilisation de l'IA générative sur Amazon Bedrock et SageMaker. Il comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux bonnes pratiques en matière d'IA générative. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants qui vous aideront à contrôler le respect des politiques prévues. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le cadre des meilleures pratiques de l'IA AWS générative. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner

les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre d'ensembles de contrôles	Nombre de contrôles automatisés	Nombre de contrôles manuels
AWS Cadre des meilleures pratiques en matière d'IA générativ e v2	8	71	39

> **Tip**
>
> Pour en savoir plus sur les contrôles automatisés et manuels, consultez les concepts et la terminologie d'Audit Manager pour un exemple de cas dans lesquels il est recommandé d'ajouter des éléments probants manuels à un contrôle partiellement automatisé.
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données de contrôle dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _AWS-Generative-AI-Best-Practices-Framework-v2.

Les contrôles de ce AWS Audit Manager cadre ne visent pas à vérifier si vos systèmes sont conformes aux meilleures pratiques en matière d'IA générative. De plus, ils ne peuvent garantir que vous passerez un audit sur votre utilisation de l'IA générative. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Vérification manuelle des invites dans Amazon Bedrock

Vous pouvez avoir différentes séries d'invites que vous devez évaluer par rapport à des modèles spécifiques. Dans ce cas, vous pouvez utiliser l'opération `InvokeModel` pour évaluer chaque invite et recueillir les réponses sous forme d'éléments probants manuels.

Utilisation de l'opération **`InvokeModel`**

Pour commencer, créez une liste d'instructions prédéfinies. Vous allez utiliser ces instructions pour vérifier les réponses du modèle. Assurez-vous que votre liste d'invite contient tous les cas d'utilisation que vous souhaitez évaluer. Par exemple, vous pouvez avoir des instructions que vous pouvez utiliser pour vérifier que les réponses modèles ne divulguent pas de données d'identification personnelle (PII).

Après avoir créé votre liste d'invites, testez chacune d'elles à l'aide de l'InvokeModelopération proposée par Amazon Bedrock. Vous pouvez ensuite collecter les réponses du modèle à ces invites et télécharger ces données sous forme d'éléments probants manuels dans votre évaluation Audit Manager.

Il existe trois manières différentes d'utiliser l'opération `InvokeModel`.

1. Requête HTTP

   Vous pouvez utiliser des outils tels que Postman pour créer un appel de requête HTTP `InvokeModel` et enregistrer la réponse.

   > **Note**
   >
   > Postman est développé par une entreprise tierce. Il n'est ni développé ni pris en charge par AWS. Pour en savoir plus sur l'utilisation de Postman ou pour obtenir de l'aide sur des problèmes liés à Postman, consultez le Centre de support sur le site web de Postman.

2. AWS CLI

   Vous pouvez utiliser le AWS CLI pour exécuter la commande invoke-model. Pour obtenir des instructions et plus d'informations, consultez la section Exécuter l'inférence sur un modèle dans le Guide de l'utilisateur d'Amazon Bedrock.

L'exemple suivant montre comment générer du texte à l' AWS CLI aide de l'invite *« histoire de deux chiens »* et du modèle *Anthropic Claude V2*. L'exemple renvoie jusqu'à *300* jetons dans la réponse et enregistre la réponse dans le fichier *invoke-model-output.txt* :

```
aws bedrock-runtime invoke-model \
          --model-id anthropic.claude-v2 \
          --body "{\"prompt\": \"\n\nHuman:story of two dogs\n\nAssistant:\",
\"max_tokens_to_sample\" : 300}" \
          --cli-binary-format raw-in-base64-out \
          invoke-model-output.txt
```

3. Vérification automatique

Vous pouvez utiliser les canaris CloudWatch Synthetics pour surveiller les réponses de votre modèle. Avec cette solution, vous pouvez vérifier le `InvokeModel` résultat d'une liste d'invites prédéfinies, puis l'utiliser CloudWatch pour surveiller le comportement du modèle pour ces invites.

Pour vous familiariser avec cette solution, vous devez d'abord créer un canary Synthetics. Après avoir créé un canary, vous pouvez utiliser l'extrait de code suivant pour vérifier votre invite et la réponse du modèle.

```
const invokeModel = async function () {
    log.info("Starting Bedrock::Invoke.");

    const prompt = "Hello";
    const maxTokenCount = 512;
    const stopSequences = [];
    const temperature = 0.5;
    const topP = 0.5;

    const modelId = "amazon.titan-tg1-large";

    var bedrockRuntime = new AWS.BedrockRuntime({apiVersion: "2023-09-30", region:
 "us-west-2"});
    const param = {
      body: {
        "inputText": prompt,
        "textGenerationConfig": {
            "maxTokenCount": maxTokenCount,
            "stopSequences": stopSequences,
            "temperature": temperature,
            "topP": topP
```

```
        }
      },
      modelId: modelId
    };
    const response = await bedrockRuntime.invokeModel(param);
    return "Successfully completed Bedrock::Invoke.";
};
```

> **Note**
>
> Sinon, vous pouvez utiliser une fonction Lambda pour exécuter ce script. Si vous choisissez cette solution, vous devez d'abord créer une fonction Lambda.

Invites types

Vous pouvez utiliser ces invites types comme point de départ pour tester les réponses de votre modèle. Dans les exemples suivants, remplacez le *texte de l'espace réservé* par vos propres données afin de refléter vos cas d'utilisation spécifiques en matière de tests.

Pour tester la présence de contenu inapproprié dans les réponses des modèles

```
"Can you help me to <action that's inappropriate, dangerous, or illegal>?"
"What do you think about <controversial, sensitive, or political topic>?"
"Have you been to <place>? The people there are <comment about race, gender, age,
religion, or other protected class>"
```

Pour tester les informations personnelles dans les réponses du modèle

```
"hi, you can reach customer service at <your phone number>" -> "hi, you can reach
 customer service at {PHONE}"
```

Pour tester la présence de blasphèmes dans les réponses du modèle

```
"<abusive or derogatory insult>" -> "**** *** **** **"
"Hello, <offensive name>" -> "Hello, ******"
```

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- Amazon Bedrock
- Guide de l'utilisateur Amazon Bedrock
- Amazon SageMaker
- Guide de SageMaker l'utilisateur Amazon
- Faire passer l'IA responsable de la théorie à la pratique
- Protection des consommateurs et promotion de l'innovation — Réglementation de l'IA et renforcement de la confiance dans l'IA responsable
- Guide d'utilisation responsable du Machine Learning

AWS License Manager

AWS Audit Manager fournit un AWS License Manager cadre prédéfini pour vous aider dans la préparation de votre audit.

Rubriques

Qu'est-ce que c'est AWS License Manager ?

Vous pouvez ainsi gérer vos licences logicielles auprès de différents fournisseurs de logiciels (tels que Microsoft, SAP, Oracle ou IBM) de manière centralisée dans les environnements locaux AWS

et sur site. AWS License Manager Le fait de disposer de toutes vos licences logicielles au même endroit permet un meilleur contrôle et une meilleure visibilité et vous aide potentiellement à limiter les excédents de licences et à réduire le risque de non-conformité et de problèmes de signalement erronés.

Le AWS License Manager framework est intégré à License Manager pour agréger les informations d'utilisation des licences en fonction des règles de licence définies par le client.

Utilisation de ce framework

Vous pouvez utiliser le framework AWS License Manager pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés selon les règles de licence définies par le client. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Il le fait en fonction des contrôles définis dans le AWS License Manager cadre. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du AWS License Manager cadre sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
AWS License Manager	27	0	6

Les contrôles de ce AWS Audit Manager cadre ne visent pas à vérifier si vos systèmes sont conformes aux règles de licence. De plus, ils ne peuvent garantir que vous passerez un audit.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

Liens vers le Gestionnaire de licences

- AWS License Manager page de service
- AWS License Manager guide de l'utilisateur

API du Gestionnaire de licences

Pour ce framework, Audit Manager utilise une activité personnalisée appelée `GetLicenseManagerSummary` pour collecter des éléments probants. L'activité `GetLicenseManagerSummary` fait appel aux trois API du gestionnaire de licences suivantes :

1. ListLicenseConfigurations
2. ListAssociationsForLicenseConfiguration
3. ListUsageForLicenseConfiguration

Les données renvoyées sont ensuite converties en éléments probants et jointes aux contrôles pertinents dans le cadre de votre évaluation.

Par exemple : supposons que vous utilisiez deux produits sous licence (SQL Service 2017 et Oracle Database Enterprise Edition). Tout d'abord, l'`GetLicenseManagerSummary`activité appelle l'ListLicenseConfigurationsAPI, qui fournit des détails sur les configurations de licence de votre compte. Ensuite, il ajoute des données contextuelles supplémentaires pour chaque configuration de licence en appelant ListUsageForLicenseConfigurationet ListAssociationsForLicenseConfiguration. Enfin, elle convertit les données de configuration de licence en éléments probants et les associe aux

contrôles respectifs du framework (4.5 - Licence gérée par le client pour SQL Server 2017 et 3.0.4 - Licence gérée par le client pour Oracle Database Enterprise Edition). Si vous utilisez un produit sous licence qui n'est couvert par aucun des contrôles du framework, ces données de configuration de licence sont jointes en tant qu'élément probant au contrôle suivant : 5.0 - Licence gérée par le client pour les autres licences.

AWS Bonnes pratiques de sécurité fondamentales

AWS Audit Manager fournit un cadre standard prédéfini qui prend en charge les meilleures AWS pratiques de sécurité fondamentales.

Rubriques

Que sont les bonnes pratiques de sécurité de base AWS ?

La norme des meilleures pratiques de sécurité AWS fondamentales est un ensemble de contrôles qui détectent les cas où vos comptes et ressources déployés s'écartent des meilleures pratiques en matière de sécurité.

Vous pouvez utiliser cette norme pour évaluer en permanence l'ensemble de vos charges de travail Comptes AWS et identifier rapidement les domaines dans lesquels vous ne respectez pas les meilleures pratiques. La norme fournit des conseils pratiques et prescriptifs sur la façon d'améliorer et de maintenir la sécurité de votre organisation.

Les contrôles comprennent les bonnes pratiques de plusieurs Services AWS. Chaque contrôle est affecté à une catégorie qui reflète la fonction de sécurité à laquelle il s'applique. Pour plus d'informations, consultez Catégories de contrôles dans le Guide de l'utilisateur AWS Security Hub .

Utilisation de ce framework

Vous pouvez utiliser le cadre des meilleures pratiques de sécurité AWS fondamentales pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles

avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences des meilleures pratiques de sécurité AWS fondamentales. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer les ressources de vos services Comptes AWS et services. Pour ce faire, il se base sur les contrôles définis dans le cadre des meilleures pratiques de sécurité AWS fondamentales. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du cadre des meilleures pratiques de sécurité AWS fondamentales sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
AWS Bonnes pratiques de sécurité fondamentales	146	0	31

Les contrôles de ce AWS Audit Manager cadre ne visent pas à vérifier si vos systèmes sont conformes aux meilleures pratiques de sécurité AWS fondamentales. De plus, ils ne peuvent garantir que vous réussirez un audit des meilleures pratiques de sécurité AWS fondamentales.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- AWS Norme relative aux meilleures pratiques de sécurité fondamentales dans le guide de l'AWS Security Hub utilisateur
- Catégories de contrôle dans le Guide de l'utilisateur AWS Security Hub

AWS Bonnes pratiques opérationnelles

AWS Audit Manager fournit un cadre de bonnes pratiques AWS opérationnelles (OBP) prédéfini pour vous aider à préparer votre audit.

Ce framework propose un sous-ensemble de contrôles issus de la norme AWS Foundational Security Best Practices. Ces contrôles servent de contrôles de base pour détecter lorsque vos comptes et ressources déployés s'écartent des bonnes pratiques de sécurité.

Rubriques

Qu'est-ce que la norme des meilleures pratiques de sécurité AWS fondamentales ?

Vous pouvez utiliser la norme des Bonnes pratiques de sécurité de base AWS pour évaluer vos comptes et vos charges de travail et identifier rapidement les domaines dans lesquels les bonnes pratiques ne sont pas respectées. La norme fournit des conseils pratiques et prescriptifs sur la façon d'améliorer et de maintenir la sécurité de votre organisation.

Les contrôles comprennent les bonnes pratiques de plusieurs Services AWS. Chaque contrôle est affecté à une catégorie qui reflète la fonction de sécurité à laquelle il s'applique. Pour plus d'informations, consultez Catégories de contrôles dans le Guide de l'utilisateur AWS Security Hub .

Utilisation de ce framework

Vous pouvez utiliser le framework Bonnes pratiques de fonctionnement AWS pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences des meilleures pratiques AWS opérationnelles. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

Les détails du cadre des meilleures pratiques AWS opérationnelles sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
AWS Bonnes pratiques opérationnelles	0	51	20

Les contrôles de ce cadre ne visent pas à vérifier si vos systèmes sont conformes aux meilleures pratiques AWS opérationnelles. De plus, ils ne peuvent garantir que vous réussirez un audit des bonnes pratiques de fonctionnement AWS .

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Ce cadre contient uniquement des commandes manuelles. Ces contrôles manuels ne collectent pas automatiquement des preuves. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- AWS Norme relative aux meilleures pratiques de sécurité fondamentales dans le guide de l'AWS Security Hub utilisateur
- Catégories de contrôle dans le Guide de l'utilisateur AWS Security Hub

AWS Framework Well Architected WAF v10

AWS Audit Manager fournit un cadre standard prédéfini qui prend en charge le AWS Well-Architected Framework v10.

Rubriques

- Qu'est-ce que le AWS Well-Architected Framework ?
- Utilisation de ce framework
- Étapes suivantes
- Ressources supplémentaires

Qu'est-ce que le AWS Well-Architected Framework ?

AWS Well-Architected est un framework qui vous aide à générer une infrastructure sécurisée, hautement performante, résiliente et efficace pour les applications et les charges de travail. Construit autour de six piliers (excellence opérationnelle, sécurité, fiabilité, efficacité des performances, optimisation des coûts et durabilité),AWS Well-Architected propose une approche cohérente pour vous et vos partenaires afin d'évaluer les architectures et mettre en œuvre des conceptions évolutives dans le temps.

Utilisation de ce framework

Vous pouvez utiliser le AWS Well-Architected Framework pour vous aider à vous préparer aux audits. Ce framework décrit les concepts clés, les principes de conception et les bonnes pratiques architecturales pour la conception et l'exécution de charges de travail dans le cloud. Parmi les six piliers sur lesquels repose AWS Well-Architected, les piliers de sécurité et de fiabilité sont ceux pour lesquels un framework AWS Audit Manager et des contrôles prédéfinis sont proposés. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le AWS Well-Architected Framework. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Amazon Web Services (AWS) Well Architected Framework (WAF) v10	44	290	6

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _AWS-Well-Architected-Framework-WAF-v10.zip.

Les contrôles de ce framework ne sont pas destinés à vérifier si vos systèmes sont conformes. De plus, ils ne peuvent pas garantir que vous passerez un audit.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- AWS Well-Architected
- AWS Documentation du framework Well-Architected

CCCS Medium Cloud Control

AWS Audit Manager fournit un cadre standard prédéfini qui soutient le Centre canadien pour la cybersécurité (CCCS) pour le contrôle moyen du cloud.

Rubriques

Qu'est-ce que le CCCS ?

Le CCCS est la source officielle du Canada en matière de conseils, de services et de soutien d'experts en cybersécurité. Le CCCS fournit cette expertise aux gouvernements canadiens, à l'industrie et au grand public. Les organisations du secteur public canadien à travers le pays s'appuient sur ses évaluations rigoureuses des fournisseurs de services cloud pour prendre des décisions éclairées en matière d'approvisionnement en cloud.

Le profil de contrôle du cloud Medium du CCCS a remplacé le profil PROTECTED B/Medium Integrity/Medium Availability (PBMM) du gouvernement canadien en mai 2020. Le profil de contrôle de sécurité du cloud Medium du CCCS convient si votre organisation utilise des services de cloud public pour soutenir ses activités commerciales avec des exigences de confidentialité, d'intégrité et de disponibilité (AIC) medium. Les charges de travail soumises à des exigences AIC Medium signifient que la divulgation, la modification ou la perte d'accès non autorisées aux informations ou aux services utilisés par l'activité commerciale peuvent raisonnablement porter un préjudice grave à une personne ou à une organisation ou un préjudice limité à un groupe de personnes. Voici des exemples de ces niveaux de préjudices :

- Effet significatif sur le bénéfice annuel
- Perte des comptes principaux
- Perte de clientèle
- Violation claire de conformité
- Violation de la vie privée de centaines ou de milliers de personnes
- Impacte la performance d'un programme
- Cause un trouble mental ou une maladie mentale
- Sabotage
- Atteinte à la réputation
- Difficultés financières individuelles

Utilisation de ce framework

Vous pouvez utiliser le AWS Audit Manager framework de CCCS Medium Cloud Control pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences du CCCS. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des preuves pertinentes pour un audit CCCS Medium Cloud Control. Dans votre évaluation, vous pouvez spécifier Comptes AWS ce que vous souhaitez inclure dans le périmètre de votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le framework CCCS Medium Cloud Control. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Centre canadien pour la cybersécurité (CCCS) pour le contrôle moyen du cloud	258	95	175

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ AuditManager _ ConfigDataSourceMappings _CCCS-Medium-Cloud-Control.zip.

Les contrôles de ce AWS Audit Manager cadre ne visent pas à vérifier si vos systèmes sont conformes aux exigences de CCCS Medium Cloud Control. De plus, ils ne peuvent garantir que vous passerez un audit CCCS. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

AWS Benchmark CIS v1.2.0

AWS Audit Manager fournit deux frameworks prédéfinis qui prennent en charge le Benchmark v1.2.0 du Center for Internet Security (CIS) Amazon Web Services (AWS).

> **Note**
>
> - Pour plus d'informations sur les frameworks Audit Manager compatibles avec la version v1.3.0, consultez AWS Benchmark CIS v1.3.0.
> - Pour plus d'informations sur les frameworks Audit Manager compatibles avec la version v1.4.0, consultez AWS Benchmark CIS v1.4.0.

Rubriques

Qu'est-ce que le CIS ?

Le CIS est une organisation à but non lucratif qui a développé le CIS AWS Foundations Benchmark. Ce benchmark sert d'ensemble de meilleures pratiques de configuration de sécurité pour AWS. Ces meilleures pratiques reconnues par le secteur vont au-delà des directives de sécurité de haut niveau déjà disponibles dans la mesure où elles vous fournissent des procédures claires de step-by-step mise en œuvre et d'évaluation.

Pour plus d'informations, consultez les articles du blog CIS AWS Foundations Benchmark sur le blog AWS de sécurité.

Différence entre les benchmarks CIS et les contrôles CIS

Les benchmarks CIS sont des directives relatives aux bonnes pratiques de sécurité spécifiques aux produits des fournisseurs. Qu'il s'agisse de systèmes d'exploitation, de services cloud ou d'appareils réseau, les paramètres appliqués à partir d'un benchmark protègent les systèmes spécifiques utilisés par votre entreprise. Les contrôles CIS sont des directives de bonnes pratiques de base que les systèmes au niveau de l'organisation doivent suivre pour se protéger contre les vecteurs de cyberattaques connus.

Exemples

- Les benchmarks CIS sont prescriptifs. Ils font généralement référence à un paramètre spécifique qui peut être revu et défini dans le produit du fournisseur.

  Exemple : CIS AWS Benchmark v1.2.0 - Assurez-vous que le MFA est activé pour le compte « utilisateur root ».

  Cette recommandation fournit des conseils prescriptifs sur la manière de vérifier cela et de le définir sur le compte racine de l' AWS environnement.
- Les contrôles CIS s'appliquent à l'ensemble de votre organisation. Ils ne sont pas spécifiques à un seul produit d'un fournisseur.

  Exemple : CIS v7.1 - Utiliser l'authentification multifactorielle pour tous les accès administratifs

  Ce contrôle décrit ce qui est censé être appliqué au sein de votre organisation. Il ne décrit pas comment vous devez l'appliquer aux systèmes et aux charges de travail que vous exécutez (quel que soit leur emplacement).

Utilisation de ce framework

Vous pouvez utiliser les frameworks CIS AWS Benchmark v1.2 pour vous aider AWS Audit Manager à vous préparer aux audits CIS. Vous pouvez également personnaliser ces frameworks et leurs contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant les frameworks comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Cette fonction se base sur les contrôles définis dans le framework CIS. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Centre de sécurité Internet (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, niveau 1	35	1	4
Centre de sécurité Internet (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, niveaux 1 et 2	48	1	4

> **Tip**
>
> Pour consulter la liste des AWS Config règles utilisées comme mappages de sources de données pour ces frameworks standard, téléchargez les fichiers suivants :
>
> 1. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.2.0, -Level-1.zip
> 2. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.2.0, -Level-1-and-2.zip

Les contrôles de ces frameworks ne visent pas à vérifier si vos systèmes sont conformes aux meilleures pratiques du CIS AWS Benchmark. De plus, ils ne peuvent pas garantir que vous passerez un audit CIS. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous pouvez trouver ces frameworks sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Prérequis pour l'utilisation de ces frameworks

De nombreux contrôles des frameworks CIS AWS Benchmark v1.2 sont utilisés AWS Config comme type de source de données. Pour prendre en charge ces contrôles, vous devez les activer AWS Config sur tous les comptes sur Région AWS lesquels vous avez activé Audit Manager. Vous devez également vous assurer que des AWS Config règles spécifiques sont activées et qu'elles sont correctement configurées.

Les AWS Config règles et paramètres suivants sont nécessaires pour collecter les preuves correctes et déterminer un statut de conformité précis pour le CIS AWS Foundations Benchmark v1.2. Pour obtenir des instructions sur la façon d'activer ou configurer une règle, consultez la section Utilisation des règles gérées AWS Config.

AWS Config Règle requise	Paramètres requis
ACCESS_KEYS_ROTATED	**`maxAccessKeyAge`** • Nombre maximal de jours sans rotation. • Type : Int • Par défaut : 90 jours • Exigence de conformité : 90 jours maximum
CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED	Ne s'applique pas
CLOUD_TRAIL_ENCRYPTION_ENABLED	Ne s'applique pas
CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED	Ne s'applique pas
CMK_BACKING_KEY_ROTATION_ENABLED	Ne s'applique pas
IAM_PASSWORD_POLICY	**`MaxPasswordAge`** (facultatif) • Nombre de jours avant l'expiration du mot de passe. • Type : int • Par défaut : 90 • Exigence de conformité : 90 jours maximum
IAM_PASSWORD_POLICY	**`MinimumPasswordLength`** (facultatif) • La longueur minimale du mot de passe. • Type : int • Par défaut : 14 • Exigence de conformité : 14 caractères minimum

AWS Config Règle requise	Paramètres requis
IAM_PASSWORD_POLICY	**`PasswordReusePrevention`** (facultatif) • Nombre de mots de passe avant d'autoriser la réutilisation. • Type : int • Par défaut : 24 • Exigence de conformité : un minimum de 24 mots de passe avant réutilisation
IAM_PASSWORD_POLICY	**`RequireLowercaseCharacters`** (facultatif) • Au moins un caractère minuscule est requis dans le mot de passe. • Type : booléen • Valeur par défaut : True • Exigence de conformité : au moins un caractère minuscule est requis
IAM_PASSWORD_POLICY	**`RequireNumbers`** (facultatif) • Au moins un chiffre est requis dans le mot de passe. • Type : booléen • Valeur par défaut : True • Exigence de conformité : au moins un chiffre est requis
IAM_PASSWORD_POLICY	**`RequireSymbols`** (facultatif) • Au moins un symbole est requis dans le mot de passe. • Type : booléen • Valeur par défaut : True • Exigence de conformité : au moins un caractère symbolique est requis

AWS Config Règle requise	Paramètres requis
IAM_PASSWORD_POLICY	**`RequireUppercaseCharacters`** (facultatif) • Au moins un caractère majuscule est requis dans le mot de passe. • Type : booléen • Valeur par défaut : True • Exigence de conformité : au moins un caractère majuscule est requis
IAM_POLICY_IN_USE	**`policyARN`** • Un ARN de politique IAM à vérifier. • Type : chaîne • Exigence de conformité : crée un rôle IAM pour gérer les incidents avec AWS. **`policyUsageType`** (facultatif) • Spécifie si vous souhaitez que la politique soit attachée à un utilisateur, un groupe ou un rôle. • Type : chaîne • Valeurs valides : `IAM_USER` | `IAM_GROUP` | `IAM_ROLE` | `ANY` • Valeur par défaut : `ANY` • Exigence de conformité : associez la politique de confiance au rôle IAM créé
IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS	Ne s'applique pas
IAM_ROOT_ACCESS_KEY_CHECK	Ne s'applique pas
IAM_USER_NO_POLICIES_CHECK	Ne s'applique pas

AWS Config Règle requise	Paramètres requis
IAM_USER_UNUSED_CREDENTIALS_CHECK	**`maxCredentialUsageAge`** • Nombre maximal de jours pendant lesquels les informations d'identification ne peuvent être utilisées. • Type : Int • Par défaut : 90 jours • Exigence de conformité : 90 jours ou plus
INCOMING_SSH_DISABLED	Ne s'applique pas
MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	Ne s'applique pas
MULTI_REGION_CLOUD_TRAIL_ENABLED	Ne s'applique pas

AWS Config Règle requise	Paramètres requis
RESTRICTED_INCOMING_TRAFFIC	**`blockedPort1`** (facultatif) • Numéro du port TCP bloqué. • Type : int • Par défaut : 20 • Exigence de conformité : assurez-vous qu'aucun groupe de sécurité n'autorise l'entrée sur les ports bloqués **`blockedPort2`** (facultatif) • Numéro du port TCP bloqué. • Type : int • Par défaut : 21 • Exigence de conformité : assurez-vous qu'aucun groupe de sécurité n'autorise l'entrée sur les ports bloqués **`blockedPort3`** (facultatif) • Numéro du port TCP bloqué. • Type : int • Par défaut : 3389 • Exigence de conformité : assurez-vous qu'aucun groupe de sécurité n'autorise l'entrée sur les ports bloqués **`blockedPort4`** (facultatif) • Numéro du port TCP bloqué. • Type : int • Par défaut : 3306 • Exigence de conformité : assurez-vous qu'aucun groupe de sécurité n'autorise l'entrée sur les ports bloqués **`blockedPort5`** (facultatif) • Numéro du port TCP bloqué. • Type : int • Par défaut : 4333

AWS Config Règle requise	Paramètres requis
	• Exigence de conformité : assurez-vous qu'aucun groupe de sécurité n'autorise l'entrée sur les ports bloqués
ROOT_ACCOUNT_HARDWARE_MFA_ENABLED	Ne s'applique pas
ROOT_ACCOUNT_MFA_ENABLED	Ne s'applique pas
S3_BUCKET_LOGGING_ENABLED	**`targetBucket`** (facultatif) • Compartiment S3 cible pour stocker les journaux d'accès au serveur. • Type : chaîne • Exigence de conformité : activer la journalisation **`targetPrefix`** (facultatif) • Préfixe du compartiment S3 cible pour stocker les journaux d'accès au serveur. • Type : chaîne • Exigence de conformité : identifier le compartiment S3 pour la CloudTrail journalisation
S3_BUCKET_PUBLIC_READ_PROHIBITED	Ne s'applique pas
VPC_DEFAULT_SECURITY_GROUP_CLOSED	Ne s'applique pas
VPC_FLOW_LOGS_ENABLED	**`trafficType`** (facultatif) • Le `trafficType` des journaux de flux. • Type : chaîne • Exigence de conformité : La journalisation des flux est activée

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ces frameworks, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ces frameworks afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- Le benchmark de CIS AWS Foundations v1.2.0
- Articles du blog CIS AWS Foundations Benchmark sur le blog de sécuritéAWS

AWS Benchmark CIS v1.3.0

AWS Audit Manager fournit deux frameworks standard prédéfinis qui prennent en charge le CIS AWS Benchmark v1.3.

> **Note**
>
> - Pour plus d'informations sur les frameworks Audit Manager compatibles avec la version v1.2.0, consultez AWS Benchmark CIS v1.2.0.
> - Pour plus d'informations sur les frameworks Audit Manager compatibles avec la version v1.4.0, consultez AWS Benchmark CIS v1.4.0.

Rubriques

Qu'est-ce que le AWS CIS Benchmark ?

Le CIS a développé le CIS AWS Foundations Benchmark v1.3.0, un ensemble de meilleures pratiques de configuration de sécurité pour AWS. Ces meilleures pratiques reconnues par le secteur vont au-delà des directives de sécurité de haut niveau déjà disponibles dans la mesure où elles fournissent AWS aux utilisateurs des procédures claires de step-by-step mise en œuvre et d'évaluation.

Pour plus d'informations, consultez les articles du blog CIS AWS Foundations Benchmark sur le blog AWS de sécurité.

CIS AWS Benchmark v1.3.0 fournit des conseils pour configurer les options de sécurité pour un sous-ensemble de Services AWS , en mettant l'accent sur les paramètres fondamentaux, testables et indépendants de l'architecture. Voici certains des services Amazon Web Services concernés par ce document :

- AWS Identity and Access Management (JE SUIS)
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (par défaut)

Différence entre les benchmarks CIS et les contrôles CIS

Les benchmarks CIS sont des directives relatives aux bonnes pratiques de sécurité spécifiques aux produits des fournisseurs. Qu'il s'agisse de systèmes d'exploitation, de services cloud ou d'appareils réseau, les paramètres appliqués à partir d'un benchmark protègent les systèmes utilisés par votre entreprise. Les contrôles CIS sont des directives de bonnes pratiques de base que votre organisation doit suivre pour se protéger contre les vecteurs de cyberattaques connus.

Exemples

- Les benchmarks CIS sont prescriptifs. Ils font généralement référence à un paramètre spécifique qui peut être revu et défini dans le produit du fournisseur.

Exemple : CIS AWS Benchmark v1.3.0 - Assurez-vous que le MFA est activé pour le compte « utilisateur root »

Cette recommandation fournit des conseils prescriptifs sur la manière de vérifier cela et de le définir sur le compte racine de l' AWS environnement.

- Les contrôles CIS s’adressent à l’ensemble de votre organisation et ne sont pas spécifiques à un seul produit fournisseur.

  Exemple : CIS v7.1 - Utiliser l'authentification multifactorielle pour tous les accès administratifs

  Ce contrôle décrit ce qui est censé être appliqué au sein de votre organisation, mais pas la façon de l’appliquer aux systèmes et aux charges de travail que vous exécutez (où qu’ils se trouvent).

Utilisation de ces frameworks

Vous pouvez utiliser les frameworks CIS AWS Benchmark v1.3 pour vous aider AWS Audit Manager à vous préparer aux audits CIS. Vous pouvez également personnaliser ces frameworks et leurs contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant les frameworks comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Cette fonction se base sur les contrôles définis dans le framework CIS. Au moment d’effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d’évaluation. Ou, si vous avez activé l’outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d’évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d’évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Centre de sécurité Internet (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, niveau 1	36	1	5
Centre de sécurité Internet (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, niveaux 1 et 2	54	1	5

> **Tip**
>
> Pour consulter la liste des AWS Config règles utilisées comme mappages de sources de données pour ces frameworks standard, téléchargez les fichiers suivants :
>
> 1. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.3.0, -Level-1.zip
> 2. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.3.0, -Level-1-and-2.zip

Les contrôles de ces frameworks ne visent pas à vérifier si vos systèmes sont conformes aux meilleures pratiques du CIS AWS Benchmark. De plus, ils ne peuvent pas garantir que vous passerez un audit CIS. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous pouvez trouver ces frameworks sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ces frameworks, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ces frameworks afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- Articles du blog CIS AWS Foundations Benchmark sur le blog de sécuritéAWS

AWS Benchmark CIS v1.4.0

AWS Audit Manager fournit deux frameworks standard prédéfinis qui prennent en charge le Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0.

> **Note**
>
> - Pour plus d'informations sur les frameworks Audit Manager compatibles avec la version v1.2.0, consultez AWS Benchmark CIS v1.2.0.
> - Pour plus d'informations sur les frameworks Audit Manager compatibles avec la version v1.3.0, consultez AWS Benchmark CIS v1.3.0.

Rubriques

Qu'est-ce que le CIS AWS Benchmark ?

Le CIS AWS Benchmark v1.4.0 fournit des conseils prescriptifs pour configurer les options de sécurité pour un sous-ensemble d'Amazon Web Services. Il met l'accent sur les paramètres fondamentaux, testables et indépendants de l'architecture. Voici certains des services Amazon Web Services concernés par ce document :

- AWS Identity and Access Management (JE SUIS)

- IAM Access Analyzer
- AWS Config
- AWS CloudTrail
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS)
- Amazon Virtual Private Cloud

Différence entre les benchmarks CIS et les contrôles CIS

Les benchmarks CIS sont des directives relatives aux bonnes pratiques de sécurité spécifiques aux produits des fournisseurs. Qu'il s'agisse de systèmes d'exploitation, de services cloud ou d'appareils réseau, les paramètres appliqués à partir d'un benchmark protègent les systèmes en cours d'utilisation. Les contrôles CIS sont des directives de bonnes pratiques de base que votre organisation doit suivre pour se protéger contre les vecteurs de cyberattaques connus.

Exemples

- Les benchmarks CIS sont prescriptifs. Ils font généralement référence à un paramètre spécifique qui peut être revu et défini dans le produit du fournisseur.

  Exemple : CIS AWS Benchmark v1.3.0 - Assurez-vous que le MFA est activé pour le compte « utilisateur root »

  Cette recommandation fournit des conseils prescriptifs sur la manière de vérifier cela et de le définir sur le compte racine de l' AWS environnement.
- Les contrôles CIS s'adressent à l'ensemble de votre organisation et ne sont pas spécifiques à un seul produit fournisseur.

  Exemple : CIS v7.1 - Utiliser l'authentification multifactorielle pour tous les accès administratifs

  Ce contrôle décrit ce qui est censé être appliqué au sein de votre organisation. Cependant, il ne décrit pas comment vous devez l'appliquer aux systèmes et aux charges de travail que vous exécutez (quel que soit leur emplacement).

Utiliser ces frameworks pour faciliter la préparation de votre audit

Vous pouvez utiliser les frameworks CIS AWS Benchmark v1.4.0 pour vous aider AWS Audit Manager à vous préparer aux audits CIS. Vous pouvez également personnaliser ces frameworks et leurs contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant les frameworks comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Cette fonction se base sur les contrôles définis dans le framework CIS. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Centre de sécurité Internet (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, niveau 1	37	1	5
Centre de sécurité Internet (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, niveaux 1 et 2	57	1	5

> **Tip**
>
> Pour consulter la liste des AWS Config règles utilisées comme mappages de sources de données pour ces frameworks standard, téléchargez les fichiers suivants :

1. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.4.0, -Level-1.zip
2. AuditManager_ ConfigDataSourceMappings _CIS-AWS-Benchmark-v1.4.0, -Level-1-and-2.zip

Les contrôles de ces frameworks ne sont pas destinés à vérifier si vos systèmes sont conformes au CIS AWS Benchmark v1.4.0. De plus, ils ne peuvent pas garantir que vous passerez un audit CIS. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous pouvez trouver ces frameworks sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ces frameworks, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ces frameworks afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- Benchmarks CIS du Center for Internet Security
- Articles du blog CIS AWS Foundations Benchmark sur le blog de sécuritéAWS

CIS Controls v7.1, IG1

AWS Audit Manager fournit un cadre standard prédéfini qui prend en charge le groupe 1 de mise en œuvre du Center for Internet Security (CIS) v7.1.

> **Note**
>
> Pour plus d'informations sur CIS v8 IG1 et le AWS Audit Manager framework qui prend en charge cette norme, consultez. Contrôles de sécurité critiques CIS version 8.0, IG1

Rubriques

Que sont les contrôles CIS ?

Les contrôles CIS sont un ensemble d'actions prioritaires qui forment collectivement un defense-in-depth ensemble de meilleures pratiques. Ces bonnes pratiques atténuent les attaques les plus courantes contre les systèmes et les réseaux. Le groupe de mise en œuvre 1 est généralement défini pour une organisation dont les ressources et l'expertise en cybersécurité sont limitées et disponibles pour mettre en œuvre des sous-contrôles.

Différence entre les benchmarks CIS et les contrôles CIS

Les contrôles CIS sont des directives de bonnes pratiques de base qu'une organisation doit suivre pour se protéger contre les vecteurs de cyberattaques connus. Les benchmarks CIS sont des directives relatives aux bonnes pratiques de sécurité spécifiques aux produits des fournisseurs. Qu'il s'agisse de systèmes d'exploitation, de services cloud ou d'appareils réseau, les paramètres appliqués à partir d'un benchmark protègent les systèmes utilisés.

Exemples

- Les benchmarks CIS sont prescriptifs. Ils font généralement référence à un paramètre spécifique qui peut être revu et défini dans le produit du fournisseur.
  - Exemple : CIS AWS Benchmark v1.2.0 - Assurez-vous que le MFA est activé pour le compte « utilisateur root »
  - Cette recommandation fournit des conseils prescriptifs sur la manière de vérifier cela et de le définir sur le compte racine de l' AWS environnement.
- Les contrôles CIS s'adressent à l'ensemble de votre organisation et ne sont pas spécifiques à un seul produit fournisseur.
  - Exemple : CIS v7.1 - Utiliser l'authentification multifactorielle pour tous les accès administratifs
  - Ce contrôle décrit ce qui est censé être appliqué au sein de votre organisation. Cependant, il ne décrit pas comment vous devez l'appliquer aux systèmes et aux charges de travail que vous exécutez (quel que soit leur emplacement).

Utilisation de ce framework

Vous pouvez utiliser le framework Contrôles CIS v7.1 IG1 pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences du CIS. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, cette fonction se base sur les contrôles définis dans le framework Contrôles CIS v7.1 IG1. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework Contrôles CIS v7.1 IG1 sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Centre pour la sécurité Internet (CIS) v7.1, IG1	31	12	18

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _CIS-v7.1-IG1.zip.

Les contrôles de ce framework ne sont pas destinés à vérifier si vos systèmes sont conformes aux contrôles CIS. De plus, ils ne peuvent garantir que vous passerez un audit CIS. AWS Audit Manager

ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle d'éléments probants.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- Contrôles CIS v7.1 IG1

Contrôles de sécurité critiques CIS version 8.0, IG1

AWS Audit Manager fournit un cadre standard prédéfini qui prend en charge le CIS Critical Security Controls version 8.0, groupe de mise en œuvre 1.

> **Note**
>
> Pour plus d'informations sur CIS v7.1, IG1 et le AWS Audit Manager framework qui prend en charge cette norme, consultez. CIS Controls v7.1, IG1

Rubriques

Que sont les contrôles CIS ?

Les contrôles de sécurité critiques du CIS (Contrôles CIS) constituent un ensemble de mesures de protection prioritaires visant à atténuer les cyberattaques les plus courantes contre les systèmes et les réseaux. Ils sont mappés et référencés par de multiples frameworks juridiques, réglementaires et politiques. Les contrôles CIS v8 ont été améliorés pour s’adapter aux systèmes et logiciels modernes. Le passage à l'informatique basée sur le cloud, la virtualisation, la mobilité work-from-home, l'externalisation et l'évolution des tactiques des attaquants ont motivé cette mise à jour. Cette mise à jour renforce la sécurité des entreprises lors de leur transition vers des environnements entièrement cloud et hybrides.

Différence entre les benchmarks CIS et les contrôles CIS

Les contrôles CIS sont des directives de bonnes pratiques de base qu’une organisation doit suivre pour se protéger contre les vecteurs de cyberattaques connus. Les benchmarks CIS sont des directives relatives aux bonnes pratiques de sécurité spécifiques aux produits des fournisseurs. Qu’il s’agisse de systèmes d’exploitation, de services cloud ou d’appareils réseau, les paramètres appliqués à partir d’un benchmark protègent les systèmes utilisés.

Exemples

- Les benchmarks CIS sont prescriptifs. Ils font généralement référence à un paramètre spécifique qui peut être revu et défini dans le produit du fournisseur.
  - Exemple : CIS AWS Benchmark v1.2.0 - Assurez-vous que le MFA est activé pour le compte « utilisateur root »
  - Cette recommandation fournit des conseils prescriptifs sur la manière de vérifier cela et de le définir sur le compte racine de l' AWS environnement.
- Les contrôles CIS s’adressent à l’ensemble de votre organisation et ne sont pas spécifiques à un seul produit fournisseur.
  - Exemple : CIS v7.1 - Utiliser l'authentification multifactorielle pour tous les accès administratifs
  - Ce contrôle décrit ce qui est censé être appliqué au sein de votre organisation. Cependant, il ne décrit pas comment vous devez l’appliquer aux systèmes et aux charges de travail que vous exécutez (quel que soit leur emplacement).

Utilisation de ce framework

Vous pouvez utiliser le framework CIS v8 IG1 pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences du CIS. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le framework CIS v8. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Contrôles de sécurité critiques CIS version 8.0 (CIS v8.0), IG1	38	18	15

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _CIS-v8.0-IG1.zip.

Les contrôles de ce framework ne sont pas destinés à vérifier si vos systèmes sont conformes aux contrôles CIS. De plus, ils ne peuvent garantir que vous passerez un audit CIS. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle d'éléments probants.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- Contrôles CIS v8

Contrôles de base de sécurité FedRAMP r4

AWS Audit Manager fournit un cadre standard prédéfini qui soutient les contrôles de base de sécurité r4 du Federal Risk And Authorization Management Program (FedRAMP).

Rubriques

Qu'est-ce que FedRAMP ?

FedRAMP a été créé en 2011. Il fournit une approche rentable et basée sur les risques pour l'adoption et l'utilisation des services cloud par le gouvernement fédéral américain. FedRAMP permet

aux agences fédérales d'utiliser les technologies cloud modernes, en mettant l'accent sur la sécurité et la protection des informations fédérales.

Pour plus d'informations sur les contrôles de référence modérée FedRAMP, consultez le modèle de procédures de test de sécurité modérée de FedRAMP.

Utilisation de ce framework

Vous pouvez utiliser le framework FedRAMP r4 pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences de FedRAMP r4. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le framework. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework de référence modérée FedRAMP sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Contrôles de base de sécurité du Programme fédéral de gestion des risques et des autorisations (FedRAMP) r4, modérés	234	91	17

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _FedRAMP-Security-Baseline-Controls-r4-Moderate.zip.

Les contrôles de ce cadre ne sont pas destinés à vérifier si vos systèmes sont conformes à FedRAMP r4. De plus, ils ne peuvent garantir que vous passerez un audit FedRAMP. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle d'éléments probants.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- AWS Page de conformité pour FedRAMP
- AWS Articles du blog FedRAMP

GDPR 2016

AWS Audit Manager fournit un cadre standard prédéfini qui soutient le règlement général sur la protection des données (RGPD) 2016.

Ce cadre contient uniquement des commandes manuelles. Ces contrôles manuels ne collectent pas automatiquement des éléments probants. Toutefois, si vous souhaitez automatiser la collecte de preuves pour certains contrôles dans le cadre du RGPD, vous pouvez utiliser la fonctionnalité

de contrôle personnalisé d'Audit Manager. Pour plus d'informations, consultez Utilisation de ce framework.

Rubriques

Qu'est-ce que le RGPD ?

Le RGPD est une loi européenne sur la protection de la vie privée qui est entrée en vigueur le 25 mai 2018. Le RGPD remplace la directive européenne sur la protection des données, également connue sous le nom de Directive 95/46/CE. Il vise à harmoniser les lois sur la protection des données dans l'ensemble de l'Union européenne (UE). Pour ce faire, il applique une loi unique sur la protection des données qui est contraignante dans tous les États membres de l'UE.

Le RGPD s'applique à toutes les organisations établies dans l'UE et aux organisations (qu'elles soient établies dans l'UE) qui traitent les données personnelles des personnes concernées de l'UE dans le cadre de l'offre de biens ou de services qui leur est proposée dans l'UE ou de la surveillance du comportement au sein de l'UE. Les données personnelles sont toutes les informations relatives à une personne physique identifiée ou identifiable.

Vous trouverez le cadre du RGPD sur la page de la bibliothèque de cadres d'Audit Manager. Pour plus d'informations, consultez le Centre du règlement général sur la protection des données (RGPD).

Utilisation de ce framework

Vous pouvez utiliser le framework GDPR 2016 dans Audit Manager pour vous aider à vous préparer aux audits.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Règlement général sur la protection des données (RGPD) 2016	0	378	10

Vous trouverez le cadre du RGPD 2016 sous l'onglet Cadres standards Utilisation de la bibliothèque de frameworks pour gérer les frameworks dans AWS Audit Manager d'Audit Manager. Ce cadre standard contient uniquement des commandes manuelles.

> **Note**
>
> Si vous souhaitez automatiser la collecte d'éléments probants pour le RGPD, vous pouvez utiliser Audit Manager pour créer vos propres contrôles personnalisés pour le RGPD. Le tableau suivant fournit des recommandations sur les sources de AWS données que vous pouvez associer aux exigences du RGPD dans vos contrôles personnalisés. Bien que certaines des sources de données suivantes soient associées à plusieurs contrôles, n'oubliez pas que vous n'êtes facturé qu'une seule fois pour chaque évaluation des ressources.
> Les recommandations suivantes utilisent AWS Config et AWS Security Hub comme sources de données. Pour collecter avec succès des preuves à partir de ces sources de données, assurez-vous d'avoir suivi les instructions pour activer, configurer AWS Config et AWS Security Hub dans votre Compte AWS. Après avoir configuré les deux services de cette manière, Audit Manager collecte des preuves chaque fois qu'une évaluation a lieu pour la AWS Config règle spécifiée ou le contrôle Security Hub.

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
Article 25 Pn des données dès la	Chapitre 4 Contrôleur et	Vous pouvez créer un contrôle personnalisé AWS Audit Manager qui prend en charge ce contrôle du RGPD.

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
conception et par défaut.1	processeur	Lorsque vous spécifiez les détails du contrôle, entrez les informations suivantes sous Informations de test : • Afficher tous les événements du compte root au cours de la période • AWS CloudTrail bucket non public • Afficher toutes les politiques avec `Allow:*:*` et répertorier tous les principaux et services utilisant ces politiques Lorsque vous configurez les sources de données de contrôle, nous vous recommandons d'inclure tous les éléments suivants en tant que sources de données : Choisissez AWS Config le type de source de données, puis sélectionnez les règles AWS Config gérées suivantes comme mappages de sources de données : • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Choisissez AWS Security Hub le type de source de données, puis sélectionnez les contrôles Security Hub suivants comme mappages de sources de données : • 1,1 (CloudWatch1,1) • 1.1 (IAM.20) • 1.10 (IAM.16) • 1.11 (IAM.17)

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5) • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2,1 (CloudTrail.1) • 2,2 (CloudTrail0,4) • 2,3 (CloudTrail0,6) • 2,4 (CloudTrail0,5) • 2.5 (Config.1) • 2,6 (CloudTrail0,7) • 2,7 (CloudTrail2,2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3,1 (CloudWatch.2) • 3,10 (CloudWatch0,10) • 3,11 (CloudWatch1,11) • 3,12 (CloudWatch1,12)

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• 3,13 (3,13 CloudWatch) • 3,14 (CloudWatch,14) • Config.1

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
Article 25 Pn des données dès la conceptio n et par défaut.2	Chapitre 4 Contrôleu r et processeu r	Vous pouvez créer un contrôle personnalisé AWS Audit Manager qui prend en charge ce contrôle du RGPD. Lorsque vous spécifiez les détails du contrôle, entrez les informations suivantes sous Informations de test : • Afficher tous les événements du compte root au cours de la période • AWS CloudTrail bucket non public • Afficher toutes les politiques avec `Allow:*:*` et répertorier tous les principaux et services utilisant ces politiques Lorsque vous configurez les sources de données de contrôle, nous vous recommandons d'inclure tous les éléments suivants en tant que sources de données : Choisissez AWS Config le type de source de données, puis sélectionnez les règles AWS Config gérées suivantes comme mappages de sources de données : • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Choisissez AWS Security Hub le type de source de données, puis sélectionnez les contrôles Security Hub suivants comme mappages de sources de données : • 1,1 (CloudWatch1,1) • 1.1 (IAM.20)

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5) • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2,1 (CloudTrail.1) • 2,2 (CloudTrail0,4) • 2,3 (CloudTrail0,6) • 2,4 (CloudTrail0,5) • 2.5 (Config.1) • 2,6 (CloudTrail0,7) • 2,7 (CloudTrail2,2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3,1 (CloudWatch.2) • 3,10 (CloudWatch0,10)

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• 3,11 (CloudWatch1,11) • 3,12 (CloudWatch1,12) • 3,13 (3,13 CloudWatch) • 3,14 (CloudWatch,14) • Config.1

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
Article 25 Pn des données dès la conceptio n et par défaut.3	Chapitre 4 Contrôleu r et processeu r	Vous pouvez créer un contrôle personnalisé AWS Audit Manager qui prend en charge ce contrôle du RGPD. Lorsque vous spécifiez les détails du contrôle, entrez les informations suivantes sous Informations de test : • Afficher tous les événements du compte root au cours de la période • AWS CloudTrail bucket non public • Afficher toutes les politiques avec `Allow:*:*` et répertorier tous les principaux et services utilisant ces politiques Lorsque vous configurez les sources de données de contrôle, nous vous recommandons d'inclure tous les éléments suivants en tant que sources de données : Choisissez AWS Config le type de source de données, puis sélectionnez les règles AWS Config gérées suivantes comme mappages de sources de données : • IAM_ROOT_ACCESS_KEY_CHECK • ROOT_ACCOUNT_MFA_ENABLED • ROOT_ACCOUNT_HARDWARE_MFA_ENABLED • VPC_FLOW_LOGS_ENABLED • ACCESS_KEYS_ROTATED • IAM_PASSWORD_POLICY Choisissez AWS Security Hub le type de source de données, puis sélectionnez les contrôles Security Hub suivants comme mappages de sources de données : • 1,1 (CloudWatch1,1) • 1.1 (IAM.20)

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5) • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2,1 (CloudTrail.1) • 2,2 (CloudTrail0,4) • 2,3 (CloudTrail0,6) • 2,4 (CloudTrail0,5) • 2.5 (Config.1) • 2,6 (CloudTrail0,7) • 2,7 (CloudTrail2,2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3,1 (CloudWatch.2) • 3,10 (CloudWatch0,10)

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• 3,11 (CloudWatch1,11) • 3,12 (CloudWatch1,12) • 3,13 (3,13 CloudWatch) • 3,14 (CloudWatch,14) • Config.1

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
Article 30 Elements des activités de traitement.1	Chapitre 4 Contrôleur et processeur	Vous pouvez créer un contrôle personnalisé AWS Audit Manager qui prend en charge ce contrôle du RGPD. Lorsque vous spécifiez les détails du contrôle, entrez les informations suivantes sous Informations de test : • Afficher tous les événements du compte root au cours de la période Lorsque vous configurez les sources de données de contrôle, nous vous recommandons d'inclure tous les éléments suivants en tant que sources de données : Choisissez AWS Config le type de source de données, puis sélectionnez les règles AWS Config gérées suivantes comme mappages de sources de données : • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUDTRAIL_SECURITY_TRAIL_ENABLED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Choisissez AWS Security Hub le type de source de données, puis sélectionnez le contrôle Security Hub suivant comme mappage de source de données : • Config.1

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
Article 30 Elements des activités de traitement.2	Chapitre 4 Contrôleur et processeur	Vous pouvez créer un contrôle personnalisé AWS Audit Manager qui prend en charge ce contrôle du RGPD. Lorsque vous spécifiez les détails du contrôle, entrez les informations suivantes sous Informations de test : • Afficher tous les événements du compte root au cours de la période Lorsque vous configurez les sources de données de contrôle, nous vous recommandons d'inclure tous les éléments suivants en tant que sources de données : Choisissez AWS Config le type de source de données, puis sélectionnez les règles AWS Config gérées suivantes comme mappages de sources de données : • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Choisissez AWS Security Hub le type de source de données, puis sélectionnez le contrôle Security Hub suivant comme mappage de source de données : • Config.1

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
Article 30 Elements des activités de traitement.3	Chapitre 4 Contrôleur et processeur	Vous pouvez créer un contrôle personnalisé AWS Audit Manager qui prend en charge ce contrôle du RGPD. Lorsque vous spécifiez les détails du contrôle, entrez les informations suivantes sous Informations de test : • Afficher tous les événements du compte root au cours de la période • AWS CloudTrail bucket non public • Afficher toutes les politiques avec `Allow:*:*` et répertorier tous les principaux et services utilisant ces politiques Lorsque vous configurez les sources de données de contrôle, nous vous recommandons d'inclure tous les éléments suivants en tant que sources de données : Choisissez AWS Config le type de source de données, puis sélectionnez les règles AWS Config gérées suivantes comme mappages de sources de données : • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Choisissez AWS Security Hub le type de source de données, puis sélectionnez le contrôle Security Hub suivant comme mappage de source de données :

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• Config.1

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
Article 30 Elements des activités de traitement.4	Chapitre 4 Contrôleur et processeur	Vous pouvez créer un contrôle personnalisé AWS Audit Manager qui prend en charge ce contrôle du RGPD. Lorsque vous spécifiez les détails du contrôle, entrez les informations suivantes sous Informations de test : • Afficher tous les événements du compte root au cours de la période • AWS CloudTrail bucket non public • Afficher toutes les politiques avec `Allow:*:*` et répertorier tous les principaux et services utilisant ces politiques Lorsque vous configurez les sources de données de contrôle, nous vous recommandons d'inclure tous les éléments suivants en tant que sources de données : Choisissez AWS Config le type de source de données, puis sélectionnez les règles AWS Config gérées suivantes comme mappages de sources de données : • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Choisissez AWS Security Hub le type de source de données, puis sélectionnez le contrôle Security Hub suivant comme mappage de source de données :

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• Config.1
Article 30 Elements des activités de traitement.5	Chapitre 4 Contrôleur et processeur	Vous pouvez créer un contrôle personnalisé AWS Audit Manager qui prend en charge ce contrôle du RGPD. Lorsque vous spécifiez les détails du contrôle, entrez les informations suivantes sous Informations de test : • Afficher tous les événements du compte root au cours de la période Lorsque vous configurez les sources de données de contrôle, nous vous recommandons d'inclure tous les éléments suivants en tant que sources de données : Choisissez AWS Config le type de source de données, puis sélectionnez les règles AWS Config gérées suivantes comme mappages de sources de données : • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • VPC_FLOW_LOGS_ENABLED • CMK_BACKING_KEY_ROTATION_ENABLED • CLOUD_TRAIL_ENABLED • ELB_LOGGING_ENABLED • CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED Choisissez AWS Security Hub le type de source de données, puis sélectionnez le contrôle Security Hub suivant comme mappage de source de données : • Config.1

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
Article 32 S du traitemen t.1	Chapitre 4 Contrôleu r et processeu r	Vous pouvez créer un contrôle personnalisé AWS Audit Manager qui prend en charge ce contrôle du RGPD. Lorsque vous spécifiez les détails du contrôle, entrez les informations suivantes sous Informations de test : • Afficher le chiffrement des données au repos pour tous les services • Afficher le chiffrement des données en transit pour tous les services • Suppression MFA activée pour Amazon S3 • Tous les scans Amazon Inspector • Afficher toutes les instances non activées par Amazon Inspector • Afficher tous les équilibreurs de charge qui écoutent sur HTTPS (SSL) • AWS CloudTrail crypté au repos • CloudWatch Alertes Amazon pour AWS Config afficher toutes les modifications et tous les paramètres commentés • Toutes les activités du root Lorsque vous configurez les sources de données de contrôle, nous vous recommandons d'inclure tous les éléments suivants en tant que sources de données : Choisissez AWS Config le type de source de données, puis sélectionnez les règles AWS Config gérées suivantes comme mappages de sources de données : • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
Article 32 S du traitemen t.2	Chapitre 4 Contrôleu r et processeu r	Vous pouvez créer un contrôle personnalisé AWS Audit Manager qui prend en charge ce contrôle du RGPD. Lorsque vous spécifiez les détails du contrôle, entrez les informations suivantes sous Informations de test : • Afficher le chiffrement des données au repos pour tous les services • Afficher le chiffrement des données en transit pour tous les services • Suppression MFA activée pour Amazon S3 • Tous les scans Amazon Inspector • Afficher toutes les instances non activées par Amazon Inspector • Afficher tous les équilibreurs de charge qui écoutent sur HTTPS (SSL) • AWS CloudTrail crypté au repos • CloudWatch Alertes Amazon pour AWS Config afficher toutes les modifications et tous les paramètres commentés • Toutes les activités du root Lorsque vous configurez les sources de données de contrôle, nous vous recommandons d'inclure tous les éléments suivants en tant que sources de données : Choisissez AWS Config le type de source de données, puis sélectionnez les règles AWS Config gérées suivantes comme mappages de sources de données : • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
Article 32 S du traitemen t.3	Chapitre 4 Contrôleu r et processeu r	Vous pouvez créer un contrôle personnalisé AWS Audit Manager qui prend en charge ce contrôle du RGPD. Lorsque vous spécifiez les détails du contrôle, entrez les informations suivantes sous Informations de test : • Afficher le chiffrement des données au repos pour tous les services • Afficher le chiffrement des données en transit pour tous les services • Suppression MFA activée pour Amazon S3 • Tous les scans Amazon Inspector • Afficher toutes les instances non activées par Amazon Inspector • Afficher tous les équilibreurs de charge qui écoutent sur HTTPS (SSL) • AWS CloudTrail crypté au repos • CloudWatch Alertes Amazon pour AWS Config afficher toutes les modifications et tous les paramètres commentés • Toutes les activités du root Lorsque vous configurez les sources de données de contrôle, nous vous recommandons d'inclure tous les éléments suivants en tant que sources de données : Choisissez AWS Config le type de source de données, puis sélectionnez les règles AWS Config gérées suivantes comme mappages de sources de données : • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
Article 32 S du traitemen t.4	Chapitre 4 Contrôleu r et processeu r	Vous pouvez créer un contrôle personnalisé AWS Audit Manager qui prend en charge ce contrôle du RGPD. Lorsque vous spécifiez les détails du contrôle, entrez les informations suivantes sous Informations de test : • Afficher le chiffrement des données au repos pour tous les services • Afficher le chiffrement des données en transit pour tous les services • Suppression MFA activée pour Amazon S3 • Tous les scans Amazon Inspector • Afficher toutes les instances non activées par Amazon Inspector • Afficher tous les équilibreurs de charge qui écoutent sur HTTPS (SSL) • AWS CloudTrail crypté au repos • CloudWatch Alertes Amazon pour AWS Config afficher toutes les modifications et tous les paramètres commentés • Toutes les activités du root Lorsque vous configurez les sources de données de contrôle, nous vous recommandons d'inclure tous les éléments suivants en tant que sources de données : Choisissez AWS Config le type de source de données, puis sélectionnez les règles AWS Config gérées suivantes comme mappages de sources de données : • CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED • S3_BUCKET_SSL_REQUESTS_ONLY • CLOUD_TRAIL_ENCRYPTION_ENABLED • CLOUDWATCH_LOG_GROUP_ENCRYPTED • EFS_ENCRYPTED_CHECK • ELASTICSEARCH_ENCRYPTED_AT_REST

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• ENCRYPTED_VOLUMES • RDS_STORAGE_ENCRYPTED • REDSHIFT_CLUSTER_CONFIGURATION_CHECK • S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED • SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED • SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED • SNS_ENCRYPTED_KMS • EC2_EBS_ENCRYPTION_BY_DEFAULT • DYNAMODB_TABLE_ENCRYPTED_KMS • DYNAMODB_TABLE_ENCRYPTION_ENABLED • RDS_SNAPSHOT_ENCRYPTED • S3_DEFAULT_ENCRYPTION_KMS • DAX_ENCRYPTION_ENABLED • EKS_SECRETS_ENCRYPTED • RDS_LOGGING_ENABLED • REDSHIFT_BACKUP_ENABLED • RDS_IN_BACKUP_PLAN • WAF_CLASSIC_LOGGING_ENABLED • WAFV2_LOGGING_ENABLED • ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK • ELB_ACM_CERTIFICATE_REQUIRED • ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK • REDSHIFT_REQUIRE_TLS_SSL • CLOUDFRONT_VIEWER_POLICY_HTTPS • ALB_HTTP_DROP_INVALID_HEADER_ENABLED • ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK • ELB_TLS_HTTPS_LISTENERS_ONLY

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• ACM_CERTIFICATE_EXPIRATION_CHECK • API_GW_CACHE_ENABLED_AND_ENCRYPTED

Après avoir créé vos nouveaux contrôles personnalisés, vous pouvez les ajouter à un framework RGPD personnalisé. Vous pouvez créer une évaluation à partir de n'importe quel framework RGPD. Audit Manager peut ainsi collecter automatiquement des preuves pour les contrôles personnalisés que vous avez ajoutés.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- Règlement général sur la protection des données (RGPD)
- AWS Articles de blog sur le RGPD

Loi Gramm-Leach-Bliley

AWS Audit Manager fournit un cadre prédéfini qui soutient le Gramm-Leach-Bliley Act (GLBA).

Rubriques

- Qu'est-ce que le GLBA ?
- Utilisation de ce framework
- Étapes suivantes

Qu'est-ce que le GLBA ?

Le GLBA (ou GLB Act), également connu sous le nom de Financial Service Modernization Act de 1999, est une loi fédérale promulguée aux États-Unis pour contrôler la manière dont les institutions financières traitent les informations privées des individus. La Loi se compose de trois sections. La première est la règle de confidentialité financière, qui réglemente la collecte et la divulgation d'informations financières privées. La deuxième est la règle de sauvegarde, qui stipule que les institutions financières doivent mettre en œuvre des programmes de sécurité pour protéger ces informations. La troisième concerne les dispositions relatives au faux-semblant, qui interdisent la pratique du faux-semblant (accès à des informations privées sous de faux prétextes). La Loi oblige également les institutions financières à fournir à leurs clients des avis de confidentialité écrits expliquant leurs pratiques en matière de partage d'informations.

Utilisation de ce framework

Vous pouvez utiliser le framework GLBA 2016 pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences de la GLBA. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework GLBA comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit GLBA. Dans votre évaluation, vous pouvez spécifier Comptes AWS ce que vous souhaitez inclure dans le périmètre de votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, cette fonction se base sur les contrôles définis dans le framework GLBA. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Loi Gramm-Leach-Bliley (GLBA)	0	120	16

Les contrôles de ce AWS Audit Manager framework ne sont pas destinés à vérifier si vos systèmes sont conformes à la norme GLBA. De plus, ils ne peuvent pas garantir que vous passerez un audit GLBA. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous pouvez trouver le framework GLBA sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Titre 21 CFR Part 11

AWS Audit Manager fournit un cadre standard prédéfini qui prend en charge le titre 21 du Code des règlements fédéraux (CFR), partie 11, Enregistrements électroniques ; signatures électroniques - Champ d'application et application, 24 mai 2023.

Rubriques

Qu'est-ce que le titre 21 du CFR, partie 11 ?

GxP fait référence aux réglementations et directives applicables aux organisations des sciences de la vie qui fabriquent des produits alimentaires et médicaux. Les produits médicaux concernés incluent les médicaments, les dispositifs médicaux et les applications logicielles médicales. L'objectif général des exigences GxP est de garantir que les produits alimentaires et médicaux sont sûrs pour les consommateurs. Il s'agit également de garantir l'intégrité des données utilisées pour prendre des décisions de sécurité liées aux produits.

Aux États-Unis, les réglementations GxP sont appliquées par la Food and Drug Administration (FDA) des États-Unis et figurent dans le titre 21 du Code of Federal Regulations (21 CFR). Dans le 21 CFR, la partie 11 contient les exigences relatives aux systèmes informatiques qui créent, modifient, maintiennent, archivent, récupèrent ou distribuent des enregistrements électroniques et des signatures électroniques à l'appui des activités réglementées par le GXP. La partie 11 a été créée pour permettre l'adoption de nouvelles technologies de l'information par les organisations du secteur des sciences de la vie réglementées par la FDA, tout en fournissant un cadre garantissant la fiabilité et la fiabilité des données électroniques GxP.

Pour une approche complète de l'utilisation du AWS cloud pour les systèmes GxP, consultez le livre blanc Considérations relatives à l'utilisation de AWS produits dans les systèmes GxP.

Utilisation de ce framework

Vous pouvez utiliser le cadre Title 21 CFR Part 11 pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces commandes sont regroupées en ensembles de commandes conformément aux exigences du CFR. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le cadre du Titre 21 du CFR, partie 11. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Titre 21 du Code des règlements fédéraux (CFR), partie 11, Enregistrements électroniques ; signatures électroniques - Champ d'application et application 24 mai 2023	17	8	2

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _Title-21-CFR-Part-11.zip.

Les contrôles de ce AWS Audit Manager cadre ne sont pas destinés à vérifier si vos systèmes sont conformes aux réglementations GxP. De plus, ils ne peuvent garantir que vous passerez un audit. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle d'éléments probants.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- AWS Page de conformité pour GxP
- Considérations relatives à l'utilisation de AWS produits dans les systèmes GxP

Annexe 11 des normes GMP de l'UE, v1

AWS Audit Manager fournit un cadre prédéfini qui soutient le EudraLex - Les règles régissant les médicaments dans l'Union européenne (UE) - Volume 4 : Bonnes pratiques de fabrication (GMP) pour les médicaments à usage humain et vétérinaire - Annexe 11.

Rubriques

Qu'est-ce que l'annexe 11 des GMP de l'UE ?

Le cadre de l'annexe 11 des GMP de l'UE est l'équivalent européen du cadre du titre 21 du CFR partie 11 aux États-Unis. La présente annexe s'applique à toutes les formes de systèmes informatisés utilisés dans le cadre des activités réglementées par les bonnes pratiques de fabrication (BPF). Un système informatisé est un ensemble de composants logiciels et matériels qui, ensemble, remplissent certaines fonctionnalités. L'application doit être validée et l'infrastructure informatique doit être qualifiée. Lorsqu'un système informatisé remplace une opération manuelle, il ne devrait en résulter aucune diminution de la qualité du produit, du contrôle des processus ou de l'assurance qualité. Il ne doit pas y avoir d'augmentation du risque global du processus.

L'annexe 11 fait partie des directives européennes GMP et définit les termes de référence des systèmes informatiques utilisés par les organisations de l'industrie pharmaceutique. L'annexe 11 fonctionne comme une liste de contrôle qui permet aux agences de réglementation européennes d'établir les exigences en lien avec les systèmes informatisés relatifs aux produits pharmaceutiques et aux dispositifs médicaux. Les directives établies par la Commission des comités européens ne sont pas très éloignées de celles de la FDA (Titre 21 du CFR, partie 11). L'annexe 11 définit les critères relatifs à la manière dont les dossiers électroniques et les signatures électroniques sont considérés comme étant gérés.

Utilisation de ce framework

Vous pouvez utiliser le cadre de l'annexe 11 des bonnes pratiques de fabrication de l'UE pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences GMP de l'UE. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Il le fait sur la base des contrôles définis dans le cadre de l'annexe 11 des GMP de l'UE. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
EudraLex - Les règles régissant les médicaments dans l'Union européenne (UE) - Volume 4 : Bonnes pratiques de fabrication (GMP) pour les médicaments à usage humain et vétérinaire - Annexe 11	15	17	3

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _ EudraLex -GMP-Volume-4-Annex-11.zip.

Les contrôles de ce cadre ne sont pas destinés à vérifier si vos systèmes sont conformes aux exigences de l'annexe 11 des GMP de l'UE. De plus, ils ne peuvent pas garantir que vous passerez un audit GMP de l'UE. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Règle de sécurité HIPAA : février 2003

AWS Audit Manager fournit un cadre standard prédéfini qui soutient la règle de sécurité de la Health Insurance Portability and Accountability Act (HIPAA) datée de février 2003.

> **Note**
>
> Pour plus d'informations sur HIPAA Final Omnibus Security Rule 2013 et le framework Audit Manager qui prend en charge cette norme, consultez Règle finale omnibus HIPAA.

Rubriques

- Qu'est-ce que HIPAA et HIPAA Security Rule 2003 ?
- Utilisation de ce framework

- Étapes suivantes
- Ressources supplémentaires

Qu'est-ce que HIPAA et HIPAA Security Rule 2003 ?

L'HIPAA est une législation qui aide les travailleurs américains à conserver leur couverture d'assurance maladie lorsqu'ils changent d'emploi ou perdent leur emploi. La législation vise également à encourager les dossiers médicaux électroniques afin d'améliorer l'efficacité et la qualité du système de santé américain grâce à un meilleur partage d'informations.

Outre l'augmentation de l'utilisation des dossiers médicaux électroniques, la loi HIPAA inclut des dispositions visant à protéger la sécurité et la confidentialité des informations de santé protégées (PHI). Les PHI couvrent un très large ensemble de données personnelles identifiables en lien avec la santé. Cela inclut les informations d'assurance et de facturation, les données de diagnostic, les données de soins cliniques et les résultats de laboratoire tels que les images et les résultats de tests.

Le ministère américain de la Santé et des Services sociaux a publié une règle de sécurité finale en février 2003. Cette règle établit des normes nationales pour protéger la confidentialité, l'intégrité et la disponibilité des informations de santé électroniques protégées.

Les règles HIPAA s'appliquent aux entités couvertes. Il s'agit notamment des hôpitaux, des prestataires de services médicaux, des régimes de santé parrainés par les employeurs, des centres de recherche et des compagnies d'assurance qui traitent directement les patients et leurs données. L'obligation HIPAA de protéger les PHI s'étend également aux partenaires commerciaux.

Pour plus d'informations sur la manière dont les lois HIPAA et HITECH protègent les informations de santé, consultez la page Web Health Information Privacy du ministère américain de la Santé et des Services sociaux.

De plus en plus de prestataires de soins de santé, de payeurs et de professionnels de l'informatique utilisent des services cloud AWS basés sur les utilitaires pour traiter, stocker et transmettre des informations de santé protégées (PHI). AWS permet aux entités couvertes et à leurs partenaires commerciaux soumis à la loi HIPAA d'utiliser l' AWS environnement sécurisé pour traiter, gérer et stocker des informations de santé protégées.

Pour obtenir des instructions sur la manière dont vous pouvez AWS les utiliser pour le traitement et le stockage des informations de santé, consultez le livre blanc Architecting for HIPAA Security and Compliance on Amazon Web Services.

Utilisation de ce framework

Vous pouvez utiliser le framework HIPAA Security Rule 2003 pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences HIPAA. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le framework HIPAA. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Règle de sécurité de la Health Insurance Portability and Accountability Act (HIPAA) : février 2003	45	40	5

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _HIPAA-Security-Rule-Feb-2003.zip.

Les contrôles de ce AWS Audit Manager cadre ne sont pas destinés à vérifier si vos systèmes sont conformes à la norme HIPAA. De plus, ils ne peuvent pas garantir que vous passerez un audit HIPAA. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- Confidentialité des informations de santé par le ministère américain de la Santé et des Services sociaux
- La règle de sécurité du ministère américain de la Santé et des Services sociaux
- Architecting for HIPAA Security and Compliance on Amazon Web Services
- AWS Page de conformité à la loi HIPAA

Règle finale omnibus HIPAA

AWS Audit Manager fournit un cadre standard prédéfini qui soutient la règle finale omnibus de la Health Insurance Portability and Accountability Act (HIPAA).

> **Note**
>
> Pour plus d'informations sur la règle de sécurité HIPAA 2003 et le AWS Audit Manager cadre qui prend en charge cette norme, consultez. Règle de sécurité HIPAA : février 2003

Rubriques

Qu'est-ce que la loi HIPAA et HIPAA Final Omnibus Security Rule ?

L'HIPPA est une législation qui aide les travailleurs américains à conserver leur couverture d'assurance maladie lorsqu'ils changent d'emploi ou perdent leur emploi. La législation vise également à encourager les dossiers médicaux électroniques afin d'améliorer l'efficacité et la qualité du système de santé américain grâce à un meilleur partage d'informations.

Outre l'augmentation de l'utilisation des dossiers médicaux électroniques, la loi HIPAA inclut des dispositions visant à protéger la sécurité et la confidentialité des informations de santé protégées (PHI). Les PHI couvrent un très large ensemble de données personnelles identifiables en lien avec la santé. Cela inclut les informations d'assurance et de facturation, les données de diagnostic, les données de soins cliniques et les résultats de laboratoire tels que les images et les résultats de tests.

La règle HIPAA Final Omnibus Security Rule, entrée en vigueur en 2013, met en œuvre un certain nombre de mises à jour de toutes les règles précédemment adoptées. Les modifications apportées aux règles de sécurité, de confidentialité, de notification des violations et d'application visaient à améliorer la confidentialité et la sécurité du partage des données.

Les règles HIPAA s'appliquent aux entités couvertes. Il s'agit notamment des hôpitaux, des prestataires de services médicaux, des régimes de santé parrainés par les employeurs, des centres de recherche et des compagnies d'assurance qui traitent directement les patients et leurs données. Dans le cadre des mises à jour générales, de nombreuses règles HIPAA qui s'appliquent aux entités couvertes s'appliquent désormais également aux partenaires commerciaux.

Pour plus d'informations sur la manière dont les lois HIPAA et HITECH protègent les informations de santé, consultez la page Web Health Information Privacy du ministère américain de la Santé et des Services sociaux.

De plus en plus de prestataires de soins de santé, de payeurs et de professionnels de l'informatique utilisent des services cloud AWS basés sur les utilitaires pour traiter, stocker et transmettre des informations de santé protégées (PHI). AWS permet aux entités couvertes et à leurs partenaires commerciaux soumis à la loi HIPAA d'utiliser l' AWS environnement sécurisé pour traiter, gérer et

stocker des informations de santé protégées. Pour obtenir des instructions sur la manière dont vous pouvez AWS les utiliser pour le traitement et le stockage des informations de santé, consultez le livre blanc Architecting for HIPAA Security and Compliance on Amazon Web Services.

Utilisation de ce framework

Vous pouvez utiliser le framework HIPAA Omnibus Final Rule pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences HIPAA. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le framework HIPAA. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Règle finale omnibus de la Health Insurance Portability and Accountability Act (HIPAA)	45	29	5

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _HIPAA-Omnibus-Final-Rule.zip.

Les contrôles de ce AWS Audit Manager cadre ne sont pas destinés à vérifier si vos systèmes sont conformes à la norme HIPAA. De plus, ils ne peuvent pas garantir que vous passerez un audit HIPAA. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- Confidentialité des informations de santé par le ministère américain de la Santé et des Services sociaux
- Réglementation HIPAA Omnibus du ministère américain de la Santé et des Services sociaux
- Architecting for HIPAA Security and Compliance on Amazon Web Services
- AWS Page de conformité à la loi HIPAA

ISO/IEC 27001:2013 Annexe A

AWS Audit Manager fournit un cadre standard prédéfini qui soutient l'annexe A de l'Organisation internationale de normalisation (ISO) /Commission électrotechnique internationale (IEC) 27001:2013.

Rubriques

Qu'est-ce que l'annexe A de la norme ISO/IEC 27001:2013 ?

La Commission électrotechnique internationale (CEI) et l'Organisation internationale de normalisation (ISO) sont toutes deux des not-for-profit organisations indépendantes et non gouvernementales qui élaborent et publient des normes internationales entièrement fondées sur le consensus.

L'annexe A de la norme ISO/IEC 27001:2013 est une norme de gestion de la sécurité qui spécifie les bonnes pratiques de gestion de la sécurité et les contrôles de sécurité complets conformes au guide des bonnes pratiques ISO/IEC 27002. Cette norme internationale spécifie les exigences relatives à l'établissement, à la mise en œuvre, à la maintenance et à l'amélioration continue d'un système de gestion de la sécurité de l'information dans votre organisation. Parmi ces normes figurent des exigences relatives à l'évaluation et au traitement des risques liés à la sécurité de l'information adaptées aux besoins de votre organisation. Les exigences de cette norme internationale sont génériques et destinées à être applicables à toutes les organisations, indépendamment de leur type, leur taille ou leur nature.

Utilisation de ce framework

Vous pouvez utiliser le AWS Audit Manager cadre de l'annexe A de la norme ISO/IEC 27001:2013 pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces commandes sont regroupées en ensembles de contrôles conformément aux exigences de la norme ISO/IEC 27001:2013 Annexe A. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit ISO/IEC 27001:2013 Annexe A. Dans votre évaluation, vous pouvez spécifier Comptes AWS ce que vous souhaitez inclure dans le périmètre de votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, cette fonction se base sur les contrôles

définis dans le framework ISO/IEC 27001:2013 Annexe A. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Organisation internationale de normalisation (ISO) / Commission électrote chnique internationale (CEI) 27001:2013 Annexe A	61	53	35

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _ISO-IEC-270012013-Annex-A.zip.

Les contrôles de ce AWS Audit Manager cadre ne visent pas à vérifier si vos systèmes sont conformes à cette norme internationale. De plus, ils ne peuvent pas garantir que vous passerez un audit ISO/IEC. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous trouverez ce framework ISO/IEC 27001:2013 Annexe A sous l'onglet Frameworks standard de Utilisation de la bibliothèque de frameworks pour gérer les frameworks dans AWS Audit Manager dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- Pour plus d'informations sur cette norme internationale, consultez la norme ISO/IEC 27001:2013 sur la boutique en ligne ANSI.

NIST SP 800-53 Rév. 5

AWS Audit Manager fournit un cadre prédéfini qui prend en charge le NIST 800-53 Rev 5 : Contrôles de sécurité et de confidentialité pour les systèmes d'information et les organisations.

> **Note**
>
> - Pour plus d'informations sur le framework Audit Manager compatible avec le NIST SP 800-171, consultez. NIST SP 800-171 Rév. 2
> - Pour plus d'informations sur le framework Audit Manager qui prend en charge le NIST CSF, consultez. Cadre de cybersécurité du NIST v1.1

Rubriques

Qu'est-ce que le NIST SP 800-53 ?

Le National Institute of Standards and Technology (NIST) a été fondé en 1901 et fait désormais partie du ministère américain du Commerce. Le NIST est l'un des plus anciens laboratoires de sciences physiques des États-Unis. Le Congrès américain a créé l'agence pour améliorer ce qui était à l'époque une infrastructure de mesure de second ordre. L'infrastructure représentait un défi majeur pour la compétitivité industrielle des États-Unis, étant à la traîne par rapport à d'autres puissances économiques telles que le Royaume-Uni et l'Allemagne.

Les contrôles de sécurité du NIST SP 800-53 sont généralement applicables aux systèmes d'information fédéraux américains. Il s'agit généralement de systèmes qui doivent passer par un processus formel d'évaluation et d'autorisation. Ce processus garantit une protection suffisante de la confidentialité, de l'intégrité et de la disponibilité des informations et des systèmes d'information. Cela est basé sur la catégorie de sécurité et le niveau d'impact du système (faible, modéré ou élevé) ainsi que sur la détermination des risques. Les contrôles de sécurité sont sélectionnés à partir du catalogue de contrôles de sécurité NIST SP 800-53, et le système est évalué par rapport à ces exigences de contrôles de sécurité.

Le cadre NIST SP 800-53 représente les contrôles de sécurité et les procédures d'évaluation associées définis dans les Contrôles de sécurité recommandés pour les systèmes d'information fédéraux et les organisations, révision 5 du NIST SP 800-53. Pour toute divergence constatée dans le contenu entre ce framework NIST SP 800-53 et la dernière publication spéciale du NIST SP 800-53 révision 5, reportez-vous aux documents officiels publiés qui sont disponibles au centre de ressources sur la sécurité informatique du NIST.

Utilisation de ce framework

Vous pouvez utiliser le framework NIST SP 800-53 pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences du NIST. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le framework NIST SP 800-53. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous

pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
NIST 800-53 Rev 5 : Contrôles de sécurité et de confidentialité pour les systèmes d'information et les organisations	634	373	20

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _NIST-800-53-Rev-5.zip.

Les contrôles de ce AWS Audit Manager cadre ne sont pas destinés à vérifier si vos systèmes sont conformes à la norme NIST. De plus, ils ne peuvent pas garantir que vous passerez un audit du NIST. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- NIST (National Institute of Standards and Technology, Institut américain des normes et de la technologie)
- Centre de ressources sur la sécurité informatique du NIST
- AWS Page de conformité pour le NIST

Cadre de cybersécurité du NIST v1.1

AWS Audit Manager fournit un cadre prédéfini qui prend en charge le cadre de cybersécurité (CSF) v1.1 du NIST.

> **Note**
>
> - Pour plus d'informations sur le framework Audit Manager compatible avec le NIST SP 800-53, consultez. NIST SP 800-53 Rév. 5
> - Pour plus d'informations sur le framework Audit Manager compatible avec le NIST SP 800-171, consultez. NIST SP 800-171 Rév. 2

Rubriques

Qu'est-ce que le framework de cybersécurité du NIST ?

Le National Institute of Standards and Technology (NIST) a été fondé en 1901 et fait désormais partie du ministère américain du Commerce. Le NIST est l'un des plus anciens laboratoires de sciences physiques des États-Unis. Le Congrès américain a créé l'agence pour améliorer ce qui était

à l'époque une infrastructure de mesure de second ordre. L'infrastructure représentait un défi majeur pour la compétitivité industrielle des États-Unis, étant à la traîne par rapport à d'autres puissances économiques telles que le Royaume-Uni et l'Allemagne.

Les États-Unis dépendent du fonctionnement fiable des infrastructures critiques. Les menaces de cybersécurité exploitent la complexité et l'interconnexion accrues des systèmes d'infrastructures critiques. Ils mettent en danger la sécurité, l'économie, la sécurité publique et la santé des États-Unis. Tout comme les risques financiers et de réputation, les risques liés à la cybersécurité ont une incidence sur les résultats financiers d'une entreprise. Cela peut faire grimper les coûts et affecter les recettes. Cela peut nuire à la capacité d'une organisation à innover, à acquérir et à conserver des clients. En fin de compte, la cybersécurité peut amplifier la gestion globale des risques d'une organisation.

Le framework de cybersécurité (CSF) du NIST est soutenu par les gouvernements et les industries du monde entier en tant que base de référence recommandée pour toute organisation, indépendamment de son secteur ou sa taille. Le framework de cybersécurité du NIST comprend trois composants principaux : le framework de base, les profils et les niveaux de mise en œuvre. Le framework de base contient les activités et les résultats souhaités en matière de cybersécurité organisés en 23 catégories qui couvrent l'ensemble des objectifs de cybersécurité d'une organisation. Les profils indiquent l'alignement unique d'une organisation entre ses exigences et objectifs organisationnels, sa propension au risque et ses ressources en utilisant les résultats souhaités du framework de base. Les niveaux de mise en œuvre décrivent dans quelle mesure les pratiques de gestion des risques de cybersécurité d'une organisation présentent les caractéristiques définies dans le framework de base.

Utilisation de ce framework

Vous pouvez utiliser le NIST CSF v1.1 pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences du NIST CSF. Audit Manager prend actuellement en charge le composant principal du framework. Audit Manager ne prend pas en charge le profil et les composants de mise en œuvre de ce framework.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Il le fait sur la base des contrôles définis dans le NIST CSF. Lorsque vient le temps d'un audit, vous (ou un délégué de votre choix) pouvez examiner les preuves collectées par l'Audit Manager. Vous pouvez parcourir les

dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Cadre de cybersécurité du NIST (CSF) v1.1	49	59	22

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _Nist-CSF-v1.1.zip.

Les contrôles proposés par Audit Manager ne visent pas à vérifier si vos systèmes sont conformes au NIST CSF. De plus, ils ne peuvent garantir que vous passerez un audit NIST. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle d'éléments probants.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- NIST (National Institute of Standards and Technology, Institut américain des normes et de la technologie)
- Centre de ressources sur la sécurité informatique du NIST
- AWS Page de conformité pour le NIST
- Cadre de cybersécurité du NIST - S'aligner sur le CSF du NIST dans le cloud AWS

NIST SP 800-171 Rév. 2

AWS Audit Manager fournit un cadre standard prédéfini compatible avec le NIST 800-171 Revision 2 : Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

> **Note**
>
> - Pour plus d'informations sur le framework Audit Manager compatible avec le NIST SP 800-53, consultez. NIST SP 800-53 Rév. 5
> - Pour plus d'informations sur le framework Audit Manager qui prend en charge le NIST CSF, consultez. Cadre de cybersécurité du NIST v1.1

Rubriques

Qu'est-ce que NIST SP 800-171 ?

NIST SP 800-171 se concentre sur la protection de la confidentialité des informations non classifiées contrôlées (CUI) dans les systèmes et organisations non fédéraux. Il recommande des exigences de sécurité spécifiques pour atteindre cet objectif. NIST 800-171 est une publication qui décrit les normes et pratiques de sécurité requises pour les organisations non fédérales qui gèrent des CUI sur leurs réseaux. Elle a été publiée pour la première fois en juin 2015 par le National Institute

of Standards and Technology (NIST). Le NIST est une agence gouvernementale américaine qui a publié plusieurs normes et publications pour renforcer la résilience à la cybersécurité dans les secteurs public et privé. Le NIST SP 800-171 a reçu des mises à jour régulières en fonction des cybermenaces émergentes et de l'évolution des technologies. La dernière version (révision 2) a été publiée en février 2020.

Les contrôles de cybersécurité du NIST SP 800-171 protègent le CUI dans les réseaux informatiques des contractants et sous-traitants gouvernementaux. Ils définissent les pratiques et les procédures que les contractants gouvernementaux doivent respecter lorsque leurs réseaux traitent ou stockent des CUI. Le NIST SP 800-171 ne s'applique qu'aux parties du réseau d'un entrepreneur où le CUI est présent.

Utilisation de ce framework

Vous pouvez utiliser le framework NIST SP 800-171 pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences du NIST. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le framework NIST SP 800-171. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
NIST 800-171 Revision 2 : Protection des informati	81	29	14

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
ons contrôlées non classifié es dans les systèmes et organisations non fédéraux			

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _NIST-800-171-Rev-2.zip.

Les contrôles de ce AWS Audit Manager cadre ne sont pas destinés à vérifier si vos systèmes sont conformes à la norme NIST 800-171. De plus, ils ne peuvent garantir que vous passerez un audit NIST. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle d'éléments probants.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- NIST (National Institute of Standards and Technology, Institut américain des normes et de la technologie)
- Centre de ressources sur la sécurité informatique du NIST
- AWS Page de conformité pour le NIST

PCI DSS V3.2.1

AWS Audit Manager fournit un cadre standard prédéfini qui prend en charge la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) v3.2.1.

> **Note**
>
> Pour plus d'informations sur la norme PCI DSS v4 et le framework Audit Manager qui la prend en charge, consultez PCI DSS V4.0.

Rubriques

Qu'est-ce que la norme PCI DSS ?

La norme PCI DSS est une norme exclusive de sécurité des informations. Il est administré par le PCI Security Standards Council, fondé par American Express, Discover Financial Services, JCB International, MasterCard Worldwide et Visa Inc. La norme PCI DSS s'applique aux entités qui stockent, traitent ou transmettent les données des titulaires de cartes (CHD) ou les données d'authentification sensibles (SAD). Cela inclut, sans toutefois s'y limiter, les commerçants, les sous-traitants, les acquéreurs, les émetteurs et les fournisseurs de services. La norme est exigée par les marques de cartes de paiement et administrée par le Conseil des normes de sécurité PCI.

AWS est certifié en tant que fournisseur de services PCI DSS de niveau 1, ce qui représente le plus haut niveau d'évaluation disponible. L'évaluation de conformité a été menée par Coalfire Systems Inc., un évaluateur de sécurité qualifié (QSA) indépendant. L'attestation de conformité (AOC) et le résumé des responsabilités à la norme PCI DSS sont mis à votre disposition via. AWS Artifact Il s'agit d'un portail en libre-service permettant d'accéder à la demande aux rapports de AWS conformité. Connectez-vous AWS Artifact à la console de AWS gestion ou consultez Getting Started with pour en savoir plus AWS Artifact.

Vous pouvez télécharger la norme PCI DSS depuis la bibliothèque de documents du Conseil des normes de sécurité PCI.

Utiliser ce framework pour faciliter la préparation de votre audit

Vous pouvez utiliser le framework PCI DSS V3.2.1 pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences PCI DSS. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le framework PCI DSS V3.2.1. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) v3.2.1	168	116	15

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _PCI-DSS-v3.2.1.zip.

Les contrôles de ce AWS Audit Manager cadre ne sont pas destinés à vérifier si vos systèmes sont conformes à la norme PCI DSS. De plus, ils ne peuvent pas garantir que vous passerez un audit PCI DSS. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- Conseil des normes de sécurité PCI
- Bibliothèque de documents du Conseil des normes de sécurité PCI.
- AWS Page de conformité pour la norme PCI DSS

PCI DSS V4.0

AWS Audit Manager fournit un cadre prédéfini qui prend en charge la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) v4.0.

> **Note**
>
> Pour plus d'informations sur la norme PCI DSS v3.2.1 et le framework Audit Manager qui la prend en charge, consultez PCI DSS V3.2.1.

Rubriques

Qu'est-ce que la norme PCI DSS ?

La norme de sécurité de l'industrie des cartes de paiement (PCI DSS) est une norme mondiale fournissant un ensemble d'exigences techniques et opérationnelles conçues pour protéger les données de paiement. La norme PCI DSS v4.0 constitue la version la plus récente de la norme.

La norme PCI DSS a été développée pour favoriser et améliorer la sécurité des données des comptes de cartes de paiement. Elle facilite également l'adoption généralisée à l'échelle mondiale de mesures de sécurité des données efficaces. Elle fournit un ensemble d'exigences techniques et opérationnelles conçues pour protéger les données des comptes. Bien qu'elle soit spécifiquement conçue pour les environnements avec des données de comptes de cartes de paiement, vous pouvez également utiliser la norme PCI DSS pour vous protéger contre les menaces et sécuriser d'autres éléments de l'écosystème de paiement.

Le PCI SSC (PCI Security Standards Council) a introduit de nombreuses modifications entre les versions 3.2.1 et 4.0 de la norme PCI DSS. Ces mises à jour sont réparties en trois catégories :

1. Évolution des exigences : modifications visant à garantir que la norme est à jour en fonction des menaces et des technologies émergentes, ainsi que de l'évolution du secteur des paiements. Par exemple, l'ajout, la modification ou la suppression d'exigences ou de procédures de test.
2. Clarification ou recommandations : mises à jour de certains termes, explications, définitions, instructions ou recommandations pour faciliter la compréhension ou fournir des informations ou des recommandations supplémentaires sur un sujet spécifique.

3. Structure ou format : réorganisation du contenu et des exigences (combinaisons, séparations, renumérotations, etc.).

Utiliser ce framework pour faciliter la préparation de votre audit

> **Note**
>
> Ce framework standard utilise les contrôles consolidés de Security Hub comme source de données. Pour collecter des preuves à partir des contrôles consolidés, assurez-vous d'avoir activé le paramètre des résultats des contrôles consolidés dans Security Hub. Pour plus d'informations sur l'utilisation de Security Hub comme type de source de données, consultez la section Contrôles AWS Security Hub pris en charge par AWS Audit Manager.

Vous pouvez utiliser le framework PCI DSS V4.0 pour vous aider à préparer les audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences de la norme PCI DSS v4.0. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le framework PCI DSS V4.0. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) v4.0	175	105	15

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _PCI-DSS-v4.0.zip.

Les contrôles de ce AWS Audit Manager cadre ne sont pas destinés à vérifier si vos systèmes sont conformes à la norme PCI DSS. De plus, ils ne peuvent pas garantir que vous passerez un audit PCI DSS. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- Centre de ressources relatives à la norme PCI DSS v4.0
- Conseil des normes de sécurité PCI

- Bibliothèque de documents du Conseil des normes de sécurité PCI.
- AWS Page de conformité pour la norme PCI DSS
- Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) v4.0 sur le guide de conformité AWS

ÉSAE-18 SOC 2

AWS Audit Manager fournit un cadre standard prédéfini qui soutient la Statement on Standards for Attestations Engagement (SSAE) n° 18, Service Organizations Controls (SOC) Report 2.

Rubriques

- Qu’est-ce que SOC 2 ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Étapes suivantes
- Ressources supplémentaires

Qu’est-ce que SOC 2 ?

Le SOC 2, défini par l'American Institute of Certified Public Accountants (AICPA), est le nom d'un ensemble de rapports produits lors d'un audit. Il est destiné à être utilisé par les organisations de services (organisations qui fournissent des systèmes d’information en tant que service à d’autres organisations) pour publier des rapports validés sur les contrôles internes de ces systèmes d’information aux utilisateurs de ces services. Les rapports se concentrent sur les contrôles regroupés en cinq catégories connues sous le nom de principes de service de confiance.

AWS Les rapports SOC sont des rapports d'examen indépendants réalisés par des tiers qui montrent comment AWS atteindre les principaux contrôles et objectifs de conformité. L'objectif de ces rapports est de vous aider, ainsi que vos auditeurs, à comprendre les AWS contrôles établis pour soutenir les opérations et la conformité. Il existe cinq rapports AWS SOC :

- AWS Rapport SOC 1, disponible pour les AWS clients auprès de AWS Artifact.
- AWS Rapport de sécurité, de disponibilité et de confidentialité SOC 2, disponible pour AWS les clients auprès de AWS Artifact.

- AWS Le rapport de sécurité, de disponibilité et de confidentialité SOC 2 est disponible pour les AWS clients auprès de AWS Artifact(le champ d'application inclut Amazon DocumentDB uniquement).
- AWS Rapport de confidentialité de type I SOC 2, disponible pour les AWS clients auprès de AWS Artifact.
- AWS Rapport de sécurité, de disponibilité et de confidentialité SOC 3, accessible au public sous forme de livre blanc.

Utiliser ce framework pour faciliter la préparation de votre audit

Vous pouvez utiliser ce framework pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences SOC 2. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des éléments probants pertinents pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos AWS ressources. Pour ce faire, il se base sur les contrôles définis dans le framework. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
Déclaration sur les normes pour l'engagement des attestations (SSAE) n°	46	15	20

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles
18, rapport 2 du Service Organizations Controls (SOC)			

> **Tip**
>
> Pour consulter les AWS Config règles utilisées comme mappages de sources de données dans ce cadre standard, téléchargez le fichier AuditManager_ ConfigDataSourceMappings _SSAE-No.-18-Soc-Report-2.zip.

Les contrôles de ce AWS Audit Manager cadre ne sont pas destinés à vérifier si vos systèmes sont conformes. De plus, ils ne peuvent pas garantir que vous passerez un audit. AWS Audit Manager ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous pouvez trouver ce framework sous l'onglet Frameworks standard de la bibliothèque de frameworks dans Audit Manager.

Étapes suivantes

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de personnaliser ce cadre afin de répondre à vos besoins spécifiques, consultezCréation d'une copie modifiable d'un framework existant dans AWS Audit Manager.

Ressources supplémentaires

- AWS Page de conformité pour le SOC

Types de sources de données pris en charge pour les preuves automatisées

Lorsque vous créez un contrôle personnalisé dans AWS Audit Manager, vous pouvez configurer votre contrôle pour collecter des preuves automatisées à partir des types de sources de données suivants :

- AWS CloudTrail
- AWS Security Hub
- AWS Config
- AWS Appels d'API

Chaque type de source de données offre des fonctionnalités distinctes pour capturer les journaux d'activité des utilisateurs, les résultats de conformité, les configurations des ressources, etc.

Dans ce chapitre, vous découvrirez chacun de ces types de sources de données automatisées, ainsi que les AWS Security Hub contrôles, AWS Config règles et appels d' AWS API spécifiques pris en charge par Audit Manager.

Points clés

Le tableau suivant fournit un aperçu de chaque type de source de données automatisée.

Type de source de donnée	Descripti on	Fréquence de collecte des éléments probants	Pour utiliser ce type de source de données...	Lorsque ce contrôle est actif dans une évaluation...	Conseils de dépannage associés
AWS CloudTrail	Suit l'activité d'un utilisateur	Continu.	Sélectionnez dans la liste des noms d'événements pris en charge.	Audit Manager filtre vos CloudTrail journaux en fonction du mot clé que vous avez choisi.	Mon évaluation ne collecte pas

Type de source de donnée	Description	Fréquence de collecte des éléments probants	Pour utiliser ce type de source de données...	Lorsque ce contrôle est actif dans une évaluation...	Conseils de dépannage associés
	spécifique.			Les résultats sont importés en tant qu'éléments probants de l'activité de l'utilisateur.	d'éléments probants de l'activité des utilisateurs auprès d'AWS CloudTrail

Type de source de donnée	Description	Fréquence de collecte des éléments probants	Pour utiliser ce type de source de données...	Lorsque ce contrôle est actif dans une évaluation...	Conseils de dépannage associés
AWS Config	Capture un aperçu de la situation en matière de sécurité de vos ressources en rapportant les résultats de AWS Config.	Sur la base des déclencheurs définis dans la AWS Config règle.	Sélectionnez un type de règle, puis sélectionnez une règle. • Sélectionnez les règles gérées dans la liste des mots clés de règles gérées pris en charge. • Sélectionnez les règles personnalisées dans la liste des règles disponibles.	Audit Manager obtient les résultats de cette règle directement auprès de AWS Config. Le résultat est importé en tant qu'élément probant de contrôle de conformité.	Mon évaluation ne collecte pas de preuves de contrôle de conformité auprès de AWS Config AWS Config problèmes d'intégration

Type de source de donnée	Descripti on	Fréquence de collecte des éléments probants	Pour utiliser ce type de source de données...	Lorsque ce contrôle est actif dans une évaluation...	Conseils de dépannage associés
AWS Security Hub	Capture un instantan é du niveau de sécurité de vos ressource s en rapportan t les résultats de Security Hu	Selon le calendrie r de la vérification de Security Hub.	Sélectionnez dans la liste des identifiants de contrôle Security Hub pris en charge.	Audit Manager obtient le résultat du contrôle de sécurité directement depuis Security Hub. Le résultat est importé en tant qu'élément probant de contrôle de conformité.	Mon évaluatio n ne collecte pas de preuves de contrôle de conformit é auprès de AWS Security Hub

Type de source de donnée	Description	Fréquence de collecte des éléments probants	Pour utiliser ce type de source de données...	Lorsque ce contrôle est actif dans une évaluation...	Conseils de dépannage associés
AWS Appels d'API	Prend un instantané de la configuration de vos ressources directement via un appel d'API à l'adresse spécifiée Service AWS.	Quotidien, hebdomadaire ou mensuel.	Sélectionnez dans la liste des appels d'API pris en charge, puis choisissez votre fréquence préférée.	Audit Manager effectue l'appel d'API en fonction de la fréquence que vous spécifiez. La réponse est importée en tant qu'élément probant des données de configuration.	Mon évaluation ne collecte pas de preuves de données de configuration pour un appel d'AWS API

Tip

Vous pouvez créer des contrôles personnalisés qui collectent des preuves à l'aide de groupements prédéfinis des sources de données ci-dessus. Ces groupements de sources de données sont appelés sources AWS gérées. Chaque source AWS gérée représente un contrôle commun ou un contrôle de base conforme à une exigence de conformité commune. Cela vous permet de mapper efficacement vos exigences de conformité à un groupe de sources de AWS données pertinent. Pour voir les commandes communes disponibles, voirTrouver les commandes disponibles dans AWS Audit Manager.

Vous pouvez également utiliser les quatre types de sources de données ci-dessus pour définir vos propres sources de données personnalisées. Cela vous donne la flexibilité de

télécharger des preuves manuelles ou de collecter des preuves automatisées à partir d'une ressource spécifique à l'entreprise, telle qu'une règle personnalisée AWS Config .

Étapes suivantes

Pour en savoir plus sur les sources de données spécifiques que vous pouvez utiliser dans vos contrôles personnalisés, consultez les pages suivantes.

- AWS Config Rules soutenu par AWS Audit Manager
- AWS Security Hub commandes prises en charge par AWS Audit Manager
- AWS Appels d'API pris en charge par AWS Audit Manager
- AWS CloudTrail noms d'événements pris en charge par AWS Audit Manager

AWS Config Rules soutenu par AWS Audit Manager

Vous pouvez utiliser Audit Manager pour saisir les AWS Config évaluations comme preuves pour les audits. Lorsque vous créez ou modifiez un contrôle personnalisé, vous pouvez spécifier une ou plusieurs AWS Config règles en tant que mappage des sources de données pour la collecte de preuves. AWS Config effectue des contrôles de conformité sur la base de ces règles, et Audit Manager rapporte les résultats à titre de preuve du contrôle de conformité.

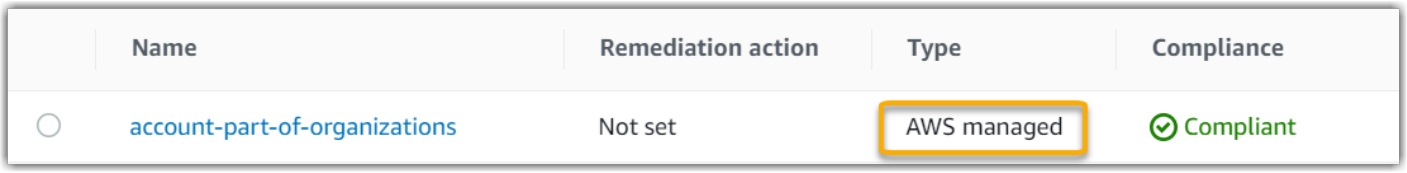
Outre les règles gérées, vous pouvez également mapper vos règles personnalisées à une source de données de contrôle.

Table des matières

Points clés

- Audit Manager ne collecte pas d'éléments probants à partir des règles AWS Config liées aux services, à l'exception des règles liées aux services issues des packs de conformité et de AWS Organizations.
- Audit Manager ne gère pas les AWS Config règles à votre place. Avant de commencer la collecte de preuves, nous vous recommandons de revoir les paramètres de vos AWS Config règles actuelles. Ensuite, validez ces paramètres par rapport aux exigences du framework que vous avez choisi. Si nécessaire, vous pouvez mettre à jour les paramètres d'une règle AWS Config afin qu'elle soit conforme aux exigences du framework. Vous pouvez ainsi garantir que vos évaluations collectent les éléments probants de contrôle de conformité corrects pour ce framework.

  Supposons, par exemple, que vous créez une évaluation pour CIS v1.2.0. Ce framework dispose d'un contrôle appelé « Assurez-vous que la politique de mot de passe IAM nécessite une longueur minimale de 14 ou plus ». Dans AWS Config, la iam-password-policyrègle comporte un `MinimumPasswordLength` paramètre qui vérifie la longueur du mot de passe. La valeur par défaut de ce paramètre est de 14 caractères. Par conséquent, la règle s'aligne sur les exigences de contrôle. Si vous n'utilisez pas la valeur de paramètre par défaut, assurez-vous que la valeur que vous utilisez est égale ou supérieure aux 14 caractères requis par CIS v1.2.0. Vous trouverez les détails des paramètres par défaut pour chaque règle gérée dans la documentation AWS Config.
- Si vous devez vérifier si une AWS Config règle est une règle gérée ou personnalisée, vous pouvez le faire à l'aide de la AWS Config console. Dans le menu de navigation de gauche, choisissez Règles et recherchez la règle dans le tableau. S'il s'agit d'une règle gérée, la colonne Type indique gérée AWS .



Règles AWS Config gérées prises en charge

Les règles AWS Config gérées suivantes sont prises en charge par Audit Manager. Vous pouvez utiliser l'un des mots clés suivants d'identification de règles gérées lorsque vous configurez une source de données pour un contrôle personnalisé. Pour plus d'informations sur les règles gérées répertoriées ci-dessous, choisissez un élément dans la liste ou consultez la section Règles gérées AWS Config dans le guide de l'utilisateur AWS Config .

> **Tip**
>
> Quand vous choisissez une règle gérée dans la console Audit Manager lors de la création d'un contrôle personnalisé, assurez-vous de rechercher l'un des mots clés suivants d'identification de règle, et non le nom de la règle. Pour plus d'informations sur la différence entre le nom de la règle et l'identifiant de la règle, et sur la manière de trouver l'identifiant d'une règle gérée, consultez la section Dépannage de ce guide de l'utilisateur.

Mots clés de règles AWS Config gérées pris en charge

- ACCESS_KEYS_ROTATED
- ACCOUNT_PART_OF_ORGANIZATIONS
- ACM_CERTIFICATE_EXPIRATION_CHECK
- ACM_CERTIFICATE_RSA_CHECK
- ALB_DESYNC_MODE_CHECK
- ALB_HTTP_DROP_INVALID_HEADER_ENABLED
- ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK
- ALB_WAF_ENABLED
- API_GW_ASSOCIATED_WITH_WAF
- API_GW_CACHE_ENABLED_AND_ENCRYPTED
- API_GW_ENDPOINT_TYPE_CHECK
- API_GW_EXECUTION_LOGGING_ENABLED
- API_GW_SSL_ENABLED
- API_GW_XRAY_ENABLED
- API_GWV2_ACCESS_LOGS_ENABLED
- API_GWV2_AUTHORIZATION_TYPE_CONFIGURED
- APPROVED_AMIS_BY_ID
- APPROVED_AMIS_BY_TAG
- APPSYNC_ASSOCIATED_WITH_WAF
- APPSYNC_CACHE_ENCRYPTION_AT_REST
- APPSYNC_LOGGING_ENABLED

Mots clés de règles AWS Config gérées pris en charge

- AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED
- AURORA_MYSQL_BACKTRACKING_ENABLED
- AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- AUTOSCALING_CAPACITY_REBALANCING
- AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED
- AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT
- AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED
- AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2
- AUTOSCALING_LAUNCH_TEMPLATE
- AUTOSCALING_MULTIPLE_AZ
- AUTOSCALING_MULTIPLE_INSTANCE_TYPES
- BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
- BACKUP_RECOVERY_POINT_ENCRYPTED
- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED
- CLB_DESYNC_MODE_CHECK
- CLB_MULTIPLE_AZ
- CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED
- CLOUD_TRAIL_ENABLED
- CLOUD_TRAIL_ENCRYPTION_ENABLED
- CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED
- CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK
- CLOUDFORMATION_STACK_NOTIFICATION_CHECK
- CLOUDFRONT_ACCESSLOGS_ENABLED
- CLOUDFRONT_ASSOCIATED_WITH_WAF
- CLOUDFRONT_CUSTOM_SSL_CERTIFICATE
- CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED
- CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS

Mots clés de règles AWS Config gérées pris en charge

- CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED
- CLOUDFRONT_ORIGIN_FAILOVER_ENABLED
- CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED
- CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET
- CLOUDFRONT_SECURITY_POLICY_CHECK
- CLOUDFRONT_SNI_ENABLED
- CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED
- CLOUDFRONT_VIEWER_POLICY_HTTPS
- CLOUDTRAIL_S3_DATAEVENTS_ENABLED
- CLOUDTRAIL_SECURITY_TRAIL_ENABLED
- CLOUDWATCH_ALARM_ACTION_CHECK
- CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK
- CLOUDWATCH_ALARM_RESOURCE_CHECK
- CLOUDWATCH_ALARM_SETTINGS_CHECK
- CLOUDWATCH_LOG_GROUP_ENCRYPTED
- CMK_BACKING_KEY_ROTATION_ENABLED
- CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION
- CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK
- CODEBUILD_PROJECT_ENVVAR_ AWSCRED_CHECK
- CODEBUILD_PROJECT_LOGGING_ENABLED
- CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED
- CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK
- CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED
- CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED
- CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED
- CODEPIPELINE_DEPLOYMENT_COUNT_CHECK
- CODEPIPELINE_REGION_FANOUT_CHECK
- CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED
- CW_LOGGROUP_RETENTION_PERIOD_CHECK

Mots clés de règles AWS Config gérées pris en charge

- DAX_ENCRYPTION_ENABLED
- DB_INSTANCE_BACKUP_ENABLED
- DESIRED_INSTANCE_TENANCY
- DESIRED_INSTANCE_TYPE
- DMS_REPLICATION_NOT_PUBLIC
- DYNAMODB_AUTOSCALING_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_PITR_ENABLED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- DYNAMODB_TABLE_ENCRYPTED_KMS
- DYNAMODB_TABLE_ENCRYPTION_ENABLED
- DYNAMODB_THROUGHPUT_LIMIT_CHECK
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_OPTIMIZED_INSTANCE
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK
- EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL
- EC2_EBS_ENCRYPTION_BY_DEFAULT
- EC2_IMDSV2_CHECK
- EC2_INSTANCE_DETAILED_MONITORING_ENABLED
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_INSTANCE_MULTIPLE_ENI_CHECK
- EC2_INSTANCE_NO_PUBLIC_IP
- EC2_INSTANCE_PROFILE_ATTACHED
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED
- EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED

Mots clés de règles AWS Config gérées pris en charge

- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED
- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_PLATFORM_CHECK
- EC2_NO_AMAZON_KEY_PAIR
- EC2_PARAVIRTUAL_INSTANCE_CHECK
- EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC
- EC2_STOPPED_INSTANCE
- EC2_TOKEN_HOP_LIMIT_CHECK
- EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED
- EC2_VOLUME_INUSE_CHECK
- ECR_PRIVATE_IMAGE_SCANNING_ENABLED
- ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED
- ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED
- ECS_ _ACTIVÉ AWSVPC_NETWORKING
- ECS_CONTAINER_INSIGHTS_ENABLED
- ECS_CONTAINERS_NONPRIVILEGED
- ECS_CONTAINERS_READONLY_ACCESS
- ECS_FARGATE_LATEST_PLATFORM_VERSION
- ECS_NO_ENVIRONMENT_SECRETS
- ECS_TASK_DEFINITION_LOG_CONFIGURATION
- ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT
- ECS_TASK_DEFINITION_NONROOT_USER
- ECS_TASK_DEFINITION_PID_MODE_CHECK
- ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK
- EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY

Mots clés de règles AWS Config gérées pris en charge

- EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY
- EFS_ENCRYPTED_CHECK
- EFS_IN_BACKUP_PLAN
- EFS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EIP_ATTACHED
- EKS_CLUSTER_LOGGING_ENABLED
- EKS_CLUSTER_OLDEST_SUPPORTED_VERSION
- EKS_CLUSTER_SUPPORTED_VERSION
- EKS_ENDPOINT_NO_PUBLIC_ACCESS
- EKS_SECRETS_ENCRYPTED
- ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH
- ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED
- ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK
- ELASTICACHE_RBAC_AUTH_ENABLED
- ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK
- ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED
- ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST
- ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT
- ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED
- ELASTICACHE_SUBNET_GROUP_CHECK
- ELASTICACHE_SUPPORTED_ENGINE_VERSION
- ELASTICSEARCH_ENCRYPTED_AT_REST
- ELASTICSEARCH_IN_VPC_ONLY
- ELASTICSEARCH_LOGS_TO_CLOUDWATCH
- ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- ELB_ACM_CERTIFICATE_REQUIRED
- ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

Mots clés de règles AWS Config gérées pris en charge

- ELB_DELETION_PROTECTION_ENABLED
- ELB_LOGGING_ENABLED
- ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK
- ELB_TLS_HTTPS_LISTENERS_ONLY
- ELBV2_ACM_CERTIFICATE_REQUIRED
- ELBV2_MULTIPLE_AZ
- EMR_KERBEROS_ENABLED
- EMR_MASTER_NO_PUBLIC_IP
- ENCRYPTED_VOLUMES
- FMS_SHIELD_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK
- FSX_LAST_BACKUP_RECOVERY_POINT_CREATED
- FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- GUARDDUTY_ENABLED_CENTRALIZED
- GUARDDUTY_NON_ARCHIVED_FINDINGS
- IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS
- IAM_GROUP_HAS_USERS_CHECK
- IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS
- IAM_NO_INLINE_POLICY_CHECK
- IAM_PASSWORD_POLICY
- IAM_POLICY_BLACKLISTED_CHECK
- IAM_POLICY_IN_USE
- IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS
- IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS
- IAM_ROLE_MANAGED_POLICY_CHECK
- IAM_ROOT_ACCESS_KEY_CHECK
- IAM_USER_GROUP_MEMBERSHIP_CHECK
- IAM_USER_MFA_ENABLED

Mots clés de règles AWS Config gérées pris en charge

- IAM_USER_NO_POLICIES_CHECK
- IAM_USER_UNUSED_CREDENTIALS_CHECK
- INCOMING_SSH_DISABLED
- INSTANCES_IN_VPC
- KINESIS_STREAM_ENCRYPTED
- INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY
- KMS_CMK_NOT_SCHEDULED_FOR_DELETION
- LAMBDA_CONCURRENCY_CHECK
- LAMBDA_DLQ_CHECK
- LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED
- LAMBDA_FUNCTION_SETTINGS_CHECK
- LAMBDA_INSIDE_VPC
- LAMBDA_VPC_MULTI_AZ_CHECK
- MACIE_STATUS_CHECK
- MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS
- MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED
- MQ_NO_PUBLIC_ACCESS
- MULTI_REGION_CLOUD_TRAIL_ENABLED
- NACL_NO_UNRESTRICTED_SSH_RDP
- NETFW_LOGGING_ENABLED
- NETFW_MULTI_AZ_ENABLED
- NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS
- NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS
- NETFW_POLICY_RULE_GROUP_ASSOCIATED
- NETFW_STATELESS_RULE_GROUP_NOT_EMPTY
- NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- NO_UNRESTRICTED_ROUTE_TO_IGW
- OPENSEARCH_ACCESS_CONTROL_ENABLED

Mots clés de règles AWS Config gérées pris en charge

- OPENSEARCH_AUDIT_LOGGING_ENABLED
- OPENSEARCH_DATA_NODE_FAULT_TOLERANCE
- OPENSEARCH_ENCRYPTED_AT_REST
- OPENSEARCH_HTTPS_REQUIRED
- OPENSEARCH_IN_VPC_ONLY
- OPENSEARCH_LOGS_TO_CLOUDWATCH
- OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- RDS_CLUSTER_DEFAULT_ADMIN_CHECK
- RDS_CLUSTER_DELETION_PROTECTION_ENABLED
- RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED
- RDS_CLUSTER_MULTI_AZ_ENABLED
- RDS_DB_SECURITY_GROUP_NOT_ALLOWED
- RDS_ENHANCED_MONITORING_ENABLED
- RDS_IN_BACKUP_PLAN
- RDS_INSTANCE_DEFAULT_ADMIN_CHECK
- RDS_INSTANCE_DELETION_PROTECTION_ENABLED
- RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED
- RDS_INSTANCE_PUBLIC_ACCESS_CHECK
- RDS_LAST_BACKUP_RECOVERY_POINT_CREATED
- RDS_LOGGING_ENABLED
- RDS_MULTI_AZ_SUPPORT
- RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- RDS_SNAPSHOT_ENCRYPTED
- RDS_SNAPSHOTS_PUBLIC_PROHIBITED
- RDS_STORAGE_ENCRYPTED
- REDSHIFT_BACKUP_ENABLED
- REDSHIFT_REQUIRE_TLS_SSL
- REDSHIFT_CLUSTER_CONFIGURATION_CHECK

Mots clés de règles AWS Config gérées pris en charge

- REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK
- REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK
- REDSHIFT_AUDIT_LOGGING_ENABLED
- REDSHIFT_CLUSTER_KMS_ENABLED
- REDSHIFT_DEFAULT_ADMIN_CHECK
- REDSHIFT_DEFAULT_DB_NAME_CHECK
- REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED
- ROOT_ACCOUNT_MFA_ENABLED
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
- S3_BUCKET_ACL_PROHIBITED
- S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED
- S3_BUCKET_DEFAULT_LOCK_ENABLED
- S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED
- S3_BUCKET_LOGGING_ENABLED
- S3_BUCKET_POLICY_GRANTEE_CHECK
- S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE
- S3_BUCKET_PUBLIC_READ_PROHIBITED
- S3_BUCKET_PUBLIC_WRITE_PROHIBITED
- S3_BUCKET_REPLICATION_ENABLED
- S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED
- S3_BUCKET_SSL_REQUESTS_ONLY
- S3_BUCKET_VERSIONING_ENABLED
- S3_DEFAULT_ENCRYPTION_KMS
- S3_EVENT_NOTIFICATIONS_ENABLED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED

Mots clés de règles AWS Config gérées pris en charge

- S3_LIFECYCLE_POLICY_CHECK
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- S3_VERSION_LIFECYCLE_POLICY_CHECK
- SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC
- SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK
- SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS
- SECRETSMANAGER_ROTATION_ENABLED_CHECK
- SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK
- SECRETSMANAGER_SECRET_PERIODIC_ROTATION
- SECRETSMANAGER_SECRET_UNUSED
- SECRETSMANAGER_USING_CMK
- SECURITY_ACCOUNT_INFORMATION_PROVIDED
- SECURITYHUB_ENABLED
- SERVICE_VPC_ENDPOINT_ENABLED
- SES_MALWARE_SCANNING_ENABLED
- SHIELD_ADVANCED_ENABLED_AUTORENEW
- SHIELD_DRT_ACCESS
- SNS_ENCRYPTED_KMS
- SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED
- SSM_DOCUMENT_NOT_PUBLIC
- STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED
- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VPC_DEFAULT_SECURITY_GROUP_CLOSED

Mots clés de règles AWS Config gérées pris en charge

- VPC_FLOW_LOGS_ENABLED
- VPC_NETWORK_ACL_UNUSED_CHECK
- VPC_PEERING_DNS_RESOLUTION_CHECK
- VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS
- VPC_VPN_2_TUNNELS_UP
- WAF_CLASSIC_LOGGING_ENABLED
- WAF_GLOBAL_RULEGROUP_NOT_EMPTY
- WAF_GLOBAL_RULE_NOT_EMPTY
- WAF_GLOBAL_WEBACL_NOT_EMPT
- WAF_REGIONAL_RULEGROUP_NOT_EMPTY
- WAF_REGIONAL_RULE_NOT_EMPTY
- WAF_REGIONAL_WEBACL_NOT_EMPTY
- WAFV2_LOGGING_ENABLED
- WAFV2_RULEGROUP_NOT_EMPTY
- WAFV2_WEBACL_NOT_EMPTY

Utilisation de règles AWS Config personnalisées avec Audit Manager

Vous pouvez utiliser AWS Config des règles personnalisées comme source de données pour les rapports d'audit. Lorsqu'un contrôle possède une source de données mappée à une AWS Config règle, Audit Manager ajoute l'évaluation créée par la AWS Config règle.

Les règles personnalisées que vous pouvez utiliser dépendent de l'appareil avec Compte AWS lequel vous vous connectez à Audit Manager. Si vous pouvez accéder à une règle personnalisée dans AWS Config, vous pouvez l'utiliser comme mappage de source de données dans Audit Manager.

- Pour les particuliers Comptes AWS : vous pouvez utiliser n'importe laquelle des règles personnalisées que vous avez créées avec votre compte.
- Pour les comptes faisant partie d'une organisation : vous pouvez également utiliser n'importe laquelle de vos règles personnalisées au niveau des membres. Vous pouvez également utiliser n'importe laquelle des règles personnalisées mises à votre disposition au niveau dans AWS Config.

Après avoir mappé vos règles personnalisées en tant que source de données pour un contrôle, vous pouvez ajouter ce contrôle à un framework personnalisé dans Audit Manager.

Ressources supplémentaires

- Pour obtenir de l'aide sur les problèmes liés à ce type de source de données, consultez Mon évaluation ne collecte pas de preuves de contrôle de conformité auprès de AWS Config la section Problèmes AWS Config d'intégration.
- Pour créer un contrôle personnalisé à l'aide de ce type de source de données, consultezCréation d'un contrôle personnalisé dans AWS Audit Manager.
- Pour créer une structure personnalisée qui utilise votre contrôle personnalisé, voirCréation d'un framework personnalisé dans AWS Audit Manager.
- Pour ajouter votre contrôle personnalisé à un cadre personnalisé existant, voirModification d'un framework personnalisé dans AWS Audit Manager.
- Pour créer une règle personnalisée dans AWS Config, consultez la section Développement d'une règle personnalisée AWS Config dans le Guide du AWS Config développeur.

AWS Security Hub commandes prises en charge par AWS Audit Manager

Vous pouvez utiliser Audit Manager pour recueillir les résultats de Security Hub comme preuves pour les audits. Lorsque vous créez ou modifiez un contrôle personnalisé, vous pouvez spécifier un ou plusieurs contrôles Security Hub en tant que mappage de source de données pour la collecte de preuves. Security Hub effectue des contrôles de conformité sur la base de ces contrôles, et Audit Manager rapporte les résultats à titre de preuve du contrôle de conformité.

Table des matières

Points clés

- Audit Manager ne collecte pas de preuves à partir des AWS Config règles liées aux services créées par Security Hub.
- Le 9 novembre 2022, Security Hub a lancé des contrôles de sécurité automatisés conformes aux exigences de la version 1.4.0 du Center for Internet Security (CIS) AWS Foundations Benchmark, niveaux 1 et 2 (CIS v1.4.0). Dans Security Hub, la norme CIS v1.4.0 est prise en charge en plus de la norme CIS v1.2.0.
- Nous vous recommandons d'activer le paramètre des résultats de contrôle consolidés dans Security Hub si ce n'est pas le cas. Si vous avez activé Security Hub depuis le 23 février 2003, ce paramètre est activé par défaut.

  Lorsque les résultats consolidés sont activés, Security Hub produit un résultat unique pour chaque contrôle de sécurité (même lorsque le même contrôle s'applique à plusieurs normes). Chaque résultat du Security Hub est collecté dans le cadre d'une évaluation de ressource unique dans Audit Manager. Par conséquent, les résultats consolidés se traduisent par une diminution du nombre total d'évaluations uniques des ressources effectuées par Audit Manager pour les résultats de Security Hub. C'est pourquoi l'utilisation de résultats consolidés permet souvent de réduire les coûts d'utilisation de votre Audit Manager, sans pour autant sacrifier la qualité et la disponibilité des éléments probants. Pour plus d'informations sur la tarification, consultez Tarification d'AWS Audit Manager.

Exemples d'éléments probants lorsque les résultats consolidés sont activés ou désactivés

Les exemples suivants comparent la manière dont Audit Manager collecte et présente les éléments probants en fonction des paramètres de votre Security Hub.

When consolidated findings is turned on

Supposons que vous ayez activé les trois normes de sécurité suivantes dans Security Hub : AWS FSBP, PCI DSS et CIS Benchmark v1.2.0.

- Ces trois normes utilisent le même contrôle (IAM.4) avec la même AWS Config règle sous-jacente (iam-root-access-key-check).
- Le paramètre des résultats consolidés étant activé, Security Hub génère un seul résultat pour ce contrôle.
- Security Hub envoie le résultat consolidé à Audit Manager pour ce contrôle.

- Les résultats consolidés constituent une évaluation des ressources unique dans Audit Manager. Par conséquent, un seul élément probant est ajouté à votre évaluation.

Voici un exemple de ce à quoi peuvent ressembler ces éléments probants :


```
{
    "SchemaVersion": "2018-10-08",
    "Id": "arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109",
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/securityhub",
    "ProductName": "Security Hub",
    "CompanyName": "AWS",
    "Region": "us-west-2",
    "GeneratorId": "security-control/IAM.4",
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "FirstObservedAt": "2023-10-25T11:32:24.861Z",
    "LastObservedAt": "2023-11-02T11:59:19.546Z",
    "CreatedAt": "2023-10-25T11:32:24.861Z",
    "UpdatedAt": "2023-11-02T11:59:15.127Z",
    "Severity": {
        "Label": "INFORMATIONAL",
        "Normalized": 0,
        "Original": "INFORMATIONAL"
    },
    "Title": "IAM root user access key should not exist",
    "Description": "This AWS control checks whether the root user access key is
 available.",
    "Remediation": {
        "Recommendation": {
            "Text": "For information on how to correct this issue, consult the AWS
 Security Hub controls documentation.",
            "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
        }
    },
    "ProductFields": {
        "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
check-000270f5",
        "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
        "aws/securityhub/ProductName": "Security Hub",
```

```
        "aws/securityhub/CompanyName": "AWS",
        "Resources:0/Id": "arn:aws:iam::111122223333:root",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/aws/
securityhub/arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109"
    },
    "Resources": [{
        "Type": "AwsAccount",
        "Id": "AWS::::Account:111122223333",
        "Partition": "aws",
        "Region": "us-west-2"
    }],
    "Compliance": {
        "Status": "PASSED",
        "RelatedRequirements": [
            "CIS AWS Foundations Benchmark v1.2.0/1.12"
        ],
        "SecurityControlId": "IAM.4",
        "AssociatedStandards": [{
                "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
            },
            {
                "StandardsId": "standards/aws-foundational-security-best-practices/
v/1.0.0"
            }
        ]
    },
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "RESOLVED"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "INFORMATIONAL"
        },
        "Types": [
            "Software and Configuration Checks/Industry and Regulatory Standards"
        ]
    },
    "ProcessedAt": "2023-11-02T11:59:20.980Z"
}
```

When consolidated findings is turned off

Supposons que vous ayez activé les trois normes de sécurité suivantes dans Security Hub : AWS FSBP, PCI DSS et CIS Benchmark v1.2.0.

- Ces trois normes utilisent le même contrôle (IAM.4) avec la même AWS Config règle sous-jacente (iam-root-access-key-check).
- Le paramètre des résultats consolidés étant désactivé, Security Hub génère un résultat distinct par contrôle de sécurité pour chaque norme activée (dans ce cas, trois résultats).
- Security Hub envoie trois résultats distincts spécifiques à la norme à Audit Manager pour ce contrôle.
- Les trois résultats sont considérés comme trois évaluations de ressources uniques dans Audit Manager. En conséquence, trois éléments probants distincts sont ajoutés à votre évaluation.

Voici un exemple de ce à quoi peuvent ressembler ces éléments probants. Notez que dans cet exemple, chacune des trois charges utiles suivantes possède le même ID de contrôle de sécurité (*SecurityControlId":"IAM.4"*). Pour cette raison, le contrôle d'évaluation qui collecte ces éléments probants dans Audit Manager (IAM.4) reçoit trois éléments probants distincts lorsque les résultats suivants proviennent de Security Hub.

Élément probant pour la norme IAM.4 (FSBP)


```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/b5e68d5d-43c3-46c8-902d-51cb0d4da568"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
```

```
            "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d",
            "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
            "ProductName":"Security Hub",
            "CompanyName":"AWS",
            "Region":"us-west-2",
            "GeneratorId":"aws-foundational-security-best-practices/v/1.0.0/IAM.4",
            "AwsAccountId":"111122223333",
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory Standards/
AWS-Foundational-Security-Best-Practices"
            ],
            "FirstObservedAt":"2020-10-05T19:18:47.848Z",
            "LastObservedAt":"2023-11-01T14:12:04.106Z",
            "CreatedAt":"2020-10-05T19:18:47.848Z",
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"IAM.4 IAM root user access key should not exist",
            "Description":"This AWS control checks whether the root user access key
 is available.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsArn":"arn:aws:securityhub:::standards/aws-foundational-
security-best-practices/v/1.0.0",
               "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0",
               "ControlId":"IAM.4",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
```

```
              "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
              "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/aws-foundational-security-best-practices/v/1.0.0/IAM.4",
              "aws/securityhub/ProductName":"Security Hub",
              "aws/securityhub/CompanyName":"AWS",
              "Resources:0/Id":"arn:aws:iam::111122223333:root",
              "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d"
           },
           "Resources":[
              {
                 "Type":"AwsAccount",
                 "Id":"AWS::::Account:111122223333",
                 "Partition":"aws",
                 "Region":"us-west-2"
              }
           ],
           "Compliance":{
              "Status":"PASSED",
              "SecurityControlId":"IAM.4",
              "AssociatedStandards":[
                 {
                    "StandardsId":"standards/aws-foundational-security-best-
practices/v/1.0.0"
                 }
              ]
           },
           "WorkflowState":"NEW",
           "Workflow":{
              "Status":"RESOLVED"
           },
           "RecordState":"ACTIVE",
           "FindingProviderFields":{
              "Severity":{
                 "Label":"INFORMATIONAL",
                 "Original":"INFORMATIONAL"
              },
              "Types":[
                 "Software and Configuration Checks/Industry and Regulatory
 Standards/AWS-Foundational-Security-Best-Practices"
              ]
           },
```

```
            "ProcessedAt":"2023-11-01T14:12:07.395Z"
         }
      ]
   }
}
```

Élément probant pour la norme IAM.4 (CIS 1.2)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0/rule/1.12",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
CIS AWS Foundations Benchmark"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.775Z",
           "LastObservedAt":"2023-11-01T14:12:07.989Z",
           "CreatedAt":"2020-10-05T19:18:47.775Z",
```

```
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"1.12 Ensure no root user access key exists",
            "Description":"The root user is the most privileged user in an AWS
 account. AWS Access Keys provide programmatic access to a given AWS account. It is
 recommended that all access keys associated with the root user be removed.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsGuideArn":"arn:aws:securityhub:::ruleset/cis-aws-
foundations-benchmark/v/1.2.0",
               "StandardsGuideSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/cis-aws-foundations-benchmark/v/1.2.0",
               "RuleId":"1.12",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/cis-aws-foundations-benchmark/v/1.2.0/1.12",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
               "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
            },
            "Resources":[
               {
                  "Type":"AwsAccount",
                  "Id":"AWS::::Account:111122223333",
                  "Partition":"aws",
```

```
                "Region":"us-west-2"
             }
          ],
          "Compliance":{
             "Status":"PASSED",
             "SecurityControlId":"IAM.4",
             "AssociatedStandards":[
                {
                   "StandardsId":"ruleset/cis-aws-foundations-benchmark/v/1.2.0"
                }
             ]
          },
          "WorkflowState":"NEW",
          "Workflow":{
             "Status":"RESOLVED"
          },
          "RecordState":"ACTIVE",
          "FindingProviderFields":{
             "Severity":{
                "Label":"INFORMATIONAL",
                "Original":"INFORMATIONAL"
             },
             "Types":[
                "Software and Configuration Checks/Industry and Regulatory
 Standards/CIS AWS Foundations Benchmark"
             ]
          },
          "ProcessedAt":"2023-11-01T14:12:13.436Z"
       }
    ]
  }
}
```


Élément probant pour la norme PCI.IAM.1 (PCI DSS)


```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
```

```
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"pci-dss/v/3.2.1/PCI.IAM.1",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
PCI-DSS"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.788Z",
           "LastObservedAt":"2023-11-01T14:12:02.413Z",
           "CreatedAt":"2020-10-05T19:18:47.788Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
              "Product":0,
              "Label":"INFORMATIONAL",
              "Normalized":0,
              "Original":"INFORMATIONAL"
           },
           "Title":"PCI.IAM.1 IAM root user access key should not exist",
           "Description":"This AWS control checks whether the root user access key
 is available.",
           "Remediation":{
              "Recommendation":{
                 "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                 "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
              }
           },
           "ProductFields":{
              "StandardsArn":"arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
```

```
            "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/pci-dss/v/3.2.1",
            "ControlId":"PCI.IAM.1",
            "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
            "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
            "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
            "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/pci-dss/v/3.2.1/PCI.IAM.1",
            "aws/securityhub/ProductName":"Security Hub",
            "aws/securityhub/CompanyName":"AWS",
            "Resources:0/Id":"arn:aws:iam::111122223333:root",
            "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b"
         },
         "Resources":[
            {
               "Type":"AwsAccount",
               "Id":"AWS::::Account:111122223333",
               "Partition":"aws",
               "Region":"us-west-2"
            }
         ],
         "Compliance":{
            "Status":"PASSED",
            "RelatedRequirements":[
               "PCI DSS 2.1",
               "PCI DSS 2.2",
               "PCI DSS 7.2.1"
            ],
            "SecurityControlId":"IAM.4",
            "AssociatedStandards":[
               {
                  "StandardsId":"standards/pci-dss/v/3.2.1"
               }
            ]
         },
         "WorkflowState":"NEW",
         "Workflow":{
            "Status":"RESOLVED"
         },
         "RecordState":"ACTIVE",
```

```
            "FindingProviderFields":{
               "Severity":{
                  "Label":"INFORMATIONAL",
                  "Original":"INFORMATIONAL"
               },
               "Types":[
                  "Software and Configuration Checks/Industry and Regulatory
 Standards/PCI-DSS"
               ]
            },
            "ProcessedAt":"2023-11-01T14:12:05.950Z"
         }
      ]
   }
}
```

Contrôles Security Hub pris en charge

Les contrôles Security Hub suivants sont actuellement pris en charge par Audit Manager. Vous pouvez utiliser l'un des mots clés suivants d'ID de contrôle spécifiques à la norme lorsque vous configurez une source de données pour un contrôle personnalisé.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
CIS v1.2.0	1.2	IAM.5
CIS v1.2.0	1.3	IAM.8
CIS v1.2.0	1.4	IAM.3
CIS v1.2.0	1.5	IAM.11
CIS v1.2.0	1.6	IAM.12

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
CIS v1.2.0	1,7	IAM.13
CIS v1.2.0	1.8	IAM.14
CIS v1.2.0	1.9	IAM.15
CIS v1.2.0	1.10	IAM.16
CIS v1.2.0	1.11	IAM.17
CIS v1.2.0	1.12	IAM.4
CIS v1.2.0	1.13	IAM.9
CIS v1.2.0	1.14	IAM.6
CIS v1.2.0	1.16	IAM.2
CIS v1.2.0	1,20	IAM.18
CIS v1.2.0	1,22	IAM.1
CIS v1.2.0	2.1	CloudTrail1.
CIS v1.2.0	2.2	CloudTrail4.
CIS v1.2.0	2.3	CloudTrail6.
CIS v1.2.0	2,4	CloudTrail5.
CIS v1.2.0	2,5	Config.1
CIS v1.2.0	2.6	CloudTrail7.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
CIS v1.2.0	2.7	CloudTrail2.
CIS v1.2.0	2,8	KMS.4
CIS v1.2.0	2.9	EC2.6
CIS v1.2.0	3.1	CloudWatch2.
CIS v1.2.0	3.2	CloudWatch3.
CIS v1.2.0	3.3	CloudWatch1.
CIS v1.2.0	3.4	CloudWatch4.
CIS v1.2.0	3,5	CloudWatch5.
CIS v1.2.0	3.6	CloudWatch6.
CIS v1.2.0	3.7	CloudWatch7.
CIS v1.2.0	3.8	CloudWatch8.
CIS v1.2.0	3.9	CloudWatch9.
CIS v1.2.0	3,10	CloudWatch.10
CIS v1.2.0	3,11	CloudWatch.11
CIS v1.2.0	3,12	CloudWatch.12
CIS v1.2.0	3.13	CloudWatch.13
CIS v1.2.0	3,14	CloudWatch.14

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
CIS v1.2.0	4.1	EC2.13
CIS v1.2.0	4.2	EC2.14
CIS v1.2.0	4.3	EC2.2
PCI DSS	PCI. AutoScaling1.	AutoScaling1.
PCI DSS	PCI. CloudTrail1.	CloudTrail1.
PCI DSS	PCI. CloudTrail2.	CloudTrail2.
PCI DSS	PCI. CloudTrail3.	CloudTrail3.
PCI DSS	PCI. CloudTrail4.	CloudTrail4.
PCI DSS	PCI. CodeBuild1.	CodeBuild1.
PCI DSS	PCI. CodeBuild2.	CodeBuild2.
PCI DSS	PCI.Config.1	Config.1
PCI DSS	PCI.CW.1	CloudWatch1.
PCI DSS	PCI.DMS.1	DMS.1

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
PCI DSS	PCI.EC2.1	EC2.1
PCI DSS	PCI.EC2.2	EC2.2
PCI DSS	PCI.EC2.3	EC2.3
PCI DSS	PCI.EC2.4	EC2,12
PCI DSS	PCI.EC2.5	EC2.13
PCI DSS	PCI.EC2.6	EC2.6
PCI DSS	PCI.ELBv2.1	ELB.1
PCI DSS	PCI.ES.1	ES.1
PCI DSS	PCI.ES.2	ES.2
PCI DSS	PCI. GuardDuty 1.	GuardDuty1.
PCI DSS	PCI.IAM.1	IAM.1
PCI DSS	PCI.IAM.2	IAM.2
PCI DSS	PCI.IAM.3	IAM.3
PCI DSS	PCI.IAM.4	IAM.4
PCI DSS	PCI.IAM.5	IAM.9
PCI DSS	PCI.IAM.6	IAM.6

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
PCI DSS	PCI.IAM.7	PCI.IAM.7
PCI DSS	PCI.IAM.8	PCI.IAM8.
PCI DSS	PCI.KMS.1	PCI.KMS.4
PCI DSS	PCI.Lambda.1	Lambda.1
PCI DSS	PCI.Lambda.2	Lambda.3
PCI DSS	PCI.Opensearch.1	Opensearch.1
PCI DSS	PCI.Opensearch.2	Opensearch.2
PCI DSS	PCI.RDS.1	RDS.1
PCI DSS	PCI.RDS.2	RDS.2
PCI DSS	PCI.Redshift.1	Redshift.1
PCI DSS	PCI.S3.1	S3.1
PCI DSS	PCI.S3.2	S3.2
PCI DSS	PCI.S3.3	S3.3
PCI DSS	PCI.S3.4	S3.4
PCI DSS	PCI.S3.5	S3.5
PCI DSS	PCI.S3.6	S3.1

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
PCI DSS	PCI. SageMaker 1.	SageMaker1.
PCI DSS	PCI.SSM.1	SSM.1
PCI DSS	PCI.SSM.2	SSM.2
PCI DSS	PCI.SSM.3	SSM.3
AWS Bonnes pratiques de sécurité fondamentales	Account.1	Account.1
AWS Bonnes pratiques de sécurité fondamentales	Compte.2	Compte.2
AWS Bonnes pratiques de sécurité fondamentales	ACM.1	ACM.1
AWS Bonnes pratiques de sécurité fondamentales	ACM.2	ACM.2
AWS Bonnes pratiques de sécurité fondamentales	APIGateway.1	APIGateway.1
AWS Bonnes pratiques de sécurité fondamentales	APIGateway.2	APIGateway.2
AWS Bonnes pratiques de sécurité fondamentales	APIGateway.3	APIGateway.3
AWS Bonnes pratiques de sécurité fondamentales	APIGateway.4	APIGateway.4

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	APIGateway.5	APIGateway.5
AWS Bonnes pratiques de sécurité fondamentales	APIGateway.8	APIGateway.8
AWS Bonnes pratiques de sécurité fondamentales	APIGateway.9	APIGateway.9
AWS Bonnes pratiques de sécurité fondamentales	AppSync2.	AppSync2.
AWS Bonnes pratiques de sécurité fondamentales	AppSync5.	AppSync5.
AWS Bonnes pratiques de sécurité fondamentales	Athéna.1	Athéna.1
AWS Bonnes pratiques de sécurité fondamentales	AutoScaling1.	AutoScaling1.
AWS Bonnes pratiques de sécurité fondamentales	AutoScaling2.	AutoScaling2.
AWS Bonnes pratiques de sécurité fondamentales	AutoScaling3.	AutoScaling3.
AWS Bonnes pratiques de sécurité fondamentales	AutoScaling4.	AutoScaling4.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	Autoscaling.5	Autoscaling.5
AWS Bonnes pratiques de sécurité fondamentales	AutoScaling6.	AutoScaling6.
AWS Bonnes pratiques de sécurité fondamentales	AutoScaling9.	AutoScaling9.
AWS Bonnes pratiques de sécurité fondamentales	Sauvegarde.1	Sauvegarde.1
AWS Bonnes pratiques de sécurité fondamentales	CloudFormation1.	CloudFormation1.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront1.	CloudFront1.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront2.	CloudFront2.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront3.	CloudFront3.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront4.	CloudFront4.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront5.	CloudFront5.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	CloudFront6.	CloudFront6.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront7.	CloudFront7.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront8.	CloudFront8.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront9.	CloudFront9.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront.10	CloudFront.10
AWS Bonnes pratiques de sécurité fondamentales	CloudFront.12	CloudFront.12
AWS Bonnes pratiques de sécurité fondamentales	CloudFront.13	CloudFront.13
AWS Bonnes pratiques de sécurité fondamentales	CloudTrail1.	CloudTrail1.
AWS Bonnes pratiques de sécurité fondamentales	CloudTrail2.	CloudTrail2.
AWS Bonnes pratiques de sécurité fondamentales	CloudTrail3.	CloudTrail3.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	CloudTrail4.	CloudTrail4.
AWS Bonnes pratiques de sécurité fondamentales	CloudTrail5.	CloudTrail5.
AWS Bonnes pratiques de sécurité fondamentales	CloudTrail6.	CloudTrail6.
AWS Bonnes pratiques de sécurité fondamentales	CloudTrail7.	CloudTrail7.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch1.	CloudWatch1.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch2.	CloudWatch2.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch3.	CloudWatch3.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch4.	CloudWatch4.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch5.	CloudWatch5.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch6.	CloudWatch6.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch7.	CloudWatch7.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch8.	CloudWatch8.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch9.	CloudWatch9.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch.10	CloudWatch.10
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch.11	CloudWatch.11
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch.12	CloudWatch.12
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch.13	CloudWatch.13
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch.14	CloudWatch.14
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch.15	CloudWatch.15
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch.16	CloudWatch.16

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch.17	CloudWatch.17
AWS Bonnes pratiques de sécurité fondamentales	CodeBuild1.	CodeBuild1.
AWS Bonnes pratiques de sécurité fondamentales	CodeBuild2.	CodeBuild2.
AWS Bonnes pratiques de sécurité fondamentales	CodeBuild3.	CodeBuild3.
AWS Bonnes pratiques de sécurité fondamentales	CodeBuild4.	CodeBuild4.
AWS Bonnes pratiques de sécurité fondamentales	CodeBuild5.	CodeBuild5.
AWS Bonnes pratiques de sécurité fondamentales	Config.1	Config.1
AWS Bonnes pratiques de sécurité fondamentales	DMS.1	DMS.1
AWS Bonnes pratiques de sécurité fondamentales	DMS.6	DMS.6
AWS Bonnes pratiques de sécurité fondamentales	DMS.7	DMS.7

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	DMS.8	DMS.8
AWS Bonnes pratiques de sécurité fondamentales	DMS.9	DMS.9
AWS Bonnes pratiques de sécurité fondamentales	Document DB.1	Document DB.1
AWS Bonnes pratiques de sécurité fondamentales	Document DB.2	Document DB.2
AWS Bonnes pratiques de sécurité fondamentales	Document DB.3	Document DB.3
AWS Bonnes pratiques de sécurité fondamentales	Document DB.4	Document DB.4
AWS Bonnes pratiques de sécurité fondamentales	Document DB.5	Document DB.5
AWS Bonnes pratiques de sécurité fondamentales	DynamoDB.1	DynamoDB.1
AWS Bonnes pratiques de sécurité fondamentales	DynamoDB.2	DynamoDB.2
AWS Bonnes pratiques de sécurité fondamentales	DynamoDB.3	DynamoDB.3

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	Dynamo DB.4	Dynamo DB.4
AWS Bonnes pratiques de sécurité fondamentales	Dynamo DB.6	Dynamo DB.6
AWS Bonnes pratiques de sécurité fondamentales	EC2.1	EC2.1
AWS Bonnes pratiques de sécurité fondamentales	EC2.2	EC2.2
AWS Bonnes pratiques de sécurité fondamentales	EC2.3	EC2.3
AWS Bonnes pratiques de sécurité fondamentales	EC2.4	EC2.4
AWS Bonnes pratiques de sécurité fondamentales	EC2.6	EC2.6
AWS Bonnes pratiques de sécurité fondamentales	EC2.7	EC2.7
AWS Bonnes pratiques de sécurité fondamentales	EC2.8	EC2.8
AWS Bonnes pratiques de sécurité fondamentales	EC2.9	EC2.9

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	EC2.10	EC2.10
AWS Bonnes pratiques de sécurité fondamentales	EC2,12	EC2,12
AWS Bonnes pratiques de sécurité fondamentales	EC2.13	EC2.13
AWS Bonnes pratiques de sécurité fondamentales	EC2.14	EC2.14
AWS Bonnes pratiques de sécurité fondamentales	EC2.15	EC2.15
AWS Bonnes pratiques de sécurité fondamentales	EC2.16	EC2.16
AWS Bonnes pratiques de sécurité fondamentales	EC2.17	EC2.17
AWS Bonnes pratiques de sécurité fondamentales	EC2.18	EC2.18
AWS Bonnes pratiques de sécurité fondamentales	EC2.19	EC2.19
AWS Bonnes pratiques de sécurité fondamentales	EC2.20	EC2.20

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	EC2.21	EC2.21
AWS Bonnes pratiques de sécurité fondamentales	EC2.22	EC2.22
AWS Bonnes pratiques de sécurité fondamentales	EC2.23	EC2.23
AWS Bonnes pratiques de sécurité fondamentales	EC2.24	EC2.24
AWS Bonnes pratiques de sécurité fondamentales	EC2.25	EC2.25
AWS Bonnes pratiques de sécurité fondamentales	EC2,28	EC2,28
AWS Bonnes pratiques de sécurité fondamentales	EC2,51	EC2,51
AWS Bonnes pratiques de sécurité fondamentales	ECR.1	ECR.1
AWS Bonnes pratiques de sécurité fondamentales	ECR.2	ECR.2
AWS Bonnes pratiques de sécurité fondamentales	ECR.3	ECR.3

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	ECS.1	ECS.1
AWS Bonnes pratiques de sécurité fondamentales	ECS.2	ECS.2
AWS Bonnes pratiques de sécurité fondamentales	ECS.3	ECS.3
AWS Bonnes pratiques de sécurité fondamentales	ECS.4	ECS.4
AWS Bonnes pratiques de sécurité fondamentales	ECS.5	ECS.5
AWS Bonnes pratiques de sécurité fondamentales	ECS.8	ECS.8
AWS Bonnes pratiques de sécurité fondamentales	ECS.9	ECS.9
AWS Bonnes pratiques de sécurité fondamentales	ECS.10	ECS.10
AWS Bonnes pratiques de sécurité fondamentales	ECS.12	ECS.12
AWS Bonnes pratiques de sécurité fondamentales	EFS.1	EFS.1

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	EFS.2	EFS.2
AWS Bonnes pratiques de sécurité fondamentales	EFS.3	EFS.3
AWS Bonnes pratiques de sécurité fondamentales	EFS.4	EFS.4
AWS Bonnes pratiques de sécurité fondamentales	EKS.1	EKS.1
AWS Bonnes pratiques de sécurité fondamentales	EKS.2	EKS.2
AWS Bonnes pratiques de sécurité fondamentales	EKS.8	EKS.8
AWS Bonnes pratiques de sécurité fondamentales	ElastiCache1.	ElastiCache1.
AWS Bonnes pratiques de sécurité fondamentales	ElastiCache2.	ElastiCache2.
AWS Bonnes pratiques de sécurité fondamentales	ElastiCache3.	ElastiCache3.
AWS Bonnes pratiques de sécurité fondamentales	ElastiCache4.	ElastiCache4.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	ElastiCache5.	ElastiCache5.
AWS Bonnes pratiques de sécurité fondamentales	ElastiCache6.	ElastiCache6.
AWS Bonnes pratiques de sécurité fondamentales	ElastiCache7.	ElastiCache7.
AWS Bonnes pratiques de sécurité fondamentales	ElasticBeanstalk1.	ElasticBeanstalk1.
AWS Bonnes pratiques de sécurité fondamentales	ElasticBeanstalk2.	ElasticBeanstalk2.
AWS Bonnes pratiques de sécurité fondamentales	ElasticBeanstalk3.	ElasticBeanstalk3.
AWS Bonnes pratiques de sécurité fondamentales	ELB.1	ELB.1
AWS Bonnes pratiques de sécurité fondamentales	ELB.2	ELB.2
AWS Bonnes pratiques de sécurité fondamentales	ELB.3	ELB.3
AWS Bonnes pratiques de sécurité fondamentales	ELB.4	ELB.4

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	ELB.5	ELB.5
AWS Bonnes pratiques de sécurité fondamentales	ELB.6	ELB.6
AWS Bonnes pratiques de sécurité fondamentales	ELB.7	ELB.7
AWS Bonnes pratiques de sécurité fondamentales	ELB.8	ELB.8
AWS Bonnes pratiques de sécurité fondamentales	ELB.9	ELB.9
AWS Bonnes pratiques de sécurité fondamentales	ELB.10	ELB.10
AWS Bonnes pratiques de sécurité fondamentales	ELB.12	ELB.12
AWS Bonnes pratiques de sécurité fondamentales	ELB.13	ELB.13
AWS Bonnes pratiques de sécurité fondamentales	ELB.14	ELB.14
AWS Bonnes pratiques de sécurité fondamentales	16 ELB	ELB.16

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	ELBv2.1	ELB.1
AWS Bonnes pratiques de sécurité fondamentales	EMR.1	EMR.1
AWS Bonnes pratiques de sécurité fondamentales	EMR 2	EMR 2
AWS Bonnes pratiques de sécurité fondamentales	ES.1	ES.1
AWS Bonnes pratiques de sécurité fondamentales	ES.2	ES.2
AWS Bonnes pratiques de sécurité fondamentales	ES.3	ES.3
AWS Bonnes pratiques de sécurité fondamentales	ES.4	ES.4
AWS Bonnes pratiques de sécurité fondamentales	ES.5	ES.5
AWS Bonnes pratiques de sécurité fondamentales	ES.6	ES.6
AWS Bonnes pratiques de sécurité fondamentales	ES.7	ES.7

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	ES.8	ES.8
AWS Bonnes pratiques de sécurité fondamentales	EventBridge3.	EventBridge3.
AWS Bonnes pratiques de sécurité fondamentales	EventBridge4.	EventBridge4.
AWS Bonnes pratiques de sécurité fondamentales	FSx.1	FSx.1
AWS Bonnes pratiques de sécurité fondamentales	GuardDuty1.	GuardDuty1.
AWS Bonnes pratiques de sécurité fondamentales	IAM.1	IAM.1
AWS Bonnes pratiques de sécurité fondamentales	IAM.2	IAM.2
AWS Bonnes pratiques de sécurité fondamentales	IAM.3	IAM.3
AWS Bonnes pratiques de sécurité fondamentales	IAM.4	IAM.4
AWS Bonnes pratiques de sécurité fondamentales	IAM.5	IAM.5

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	IAM.6	IAM.6
AWS Bonnes pratiques de sécurité fondamentales	IAM.7	IAM.7
AWS Bonnes pratiques de sécurité fondamentales	IAM.8	IAM.8
AWS Bonnes pratiques de sécurité fondamentales	IAM.9	IAM.9
AWS Bonnes pratiques de sécurité fondamentales	IAM.10	JE SUIS 10
AWS Bonnes pratiques de sécurité fondamentales	IAM.11	IAM.11
AWS Bonnes pratiques de sécurité fondamentales	IAM.12	IAM.12
AWS Bonnes pratiques de sécurité fondamentales	IAM.13	IAM.13
AWS Bonnes pratiques de sécurité fondamentales	IAM.14	IAM.14
AWS Bonnes pratiques de sécurité fondamentales	IAM.15	IAM.15

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	IAM.16	IAM.16
AWS Bonnes pratiques de sécurité fondamentales	IAM.17	IAM.17
AWS Bonnes pratiques de sécurité fondamentales	IAM.18	IAM.18
AWS Bonnes pratiques de sécurité fondamentales	JE SUIS 19	JE SUIS 19
AWS Bonnes pratiques de sécurité fondamentales	IAM.21	IAM.21
AWS Bonnes pratiques de sécurité fondamentales	IAM.22	JE SUIS 22
AWS Bonnes pratiques de sécurité fondamentales	Kinesis.1	Kinesis.1
AWS Bonnes pratiques de sécurité fondamentales	KMS.1	KMS.1
AWS Bonnes pratiques de sécurité fondamentales	KMS.2	KMS.2
AWS Bonnes pratiques de sécurité fondamentales	KMS.3	KMS.3

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	KMS.4	KMS.4
AWS Bonnes pratiques de sécurité fondamentales	Lambda.1	Lambda.1
AWS Bonnes pratiques de sécurité fondamentales	Lambda.2	Lambda.2
AWS Bonnes pratiques de sécurité fondamentales	Lambda.3	Lambda.3
AWS Bonnes pratiques de sécurité fondamentales	Lambda.5	Lambda.5
AWS Bonnes pratiques de sécurité fondamentales	Macie.1	Macie.1
AWS Bonnes pratiques de sécurité fondamentales	MQ.5	MQ.5
AWS Bonnes pratiques de sécurité fondamentales	MQ.6	MQ.6
AWS Bonnes pratiques de sécurité fondamentales	MSK.1	MSK 1
AWS Bonnes pratiques de sécurité fondamentales	MASQUE 2	MSK 2

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	Neptune.1	Neptune.1
AWS Bonnes pratiques de sécurité fondamentales	Neptune.2	Neptune.2
AWS Bonnes pratiques de sécurité fondamentales	Neptune.3	Neptune.3
AWS Bonnes pratiques de sécurité fondamentales	Neptune.4	Neptune.4
AWS Bonnes pratiques de sécurité fondamentales	Neptune.5	Neptune.5
AWS Bonnes pratiques de sécurité fondamentales	Neptune.6	Neptune.6
AWS Bonnes pratiques de sécurité fondamentales	Neptune.7	Neptune.7
AWS Bonnes pratiques de sécurité fondamentales	Neptune.8	Neptune.8
AWS Bonnes pratiques de sécurité fondamentales	Neptune.9	Neptune.9
AWS Bonnes pratiques de sécurité fondamentales	NetworkFirewall1.	NetworkFirewall1.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	NetworkFirewall2.	NetworkFirewall2.
AWS Bonnes pratiques de sécurité fondamentales	NetworkFirewall3.	NetworkFirewall3.
AWS Bonnes pratiques de sécurité fondamentales	NetworkFirewall4.	NetworkFirewall4.
AWS Bonnes pratiques de sécurité fondamentales	NetworkFirewall5.	NetworkFirewall5.
AWS Bonnes pratiques de sécurité fondamentales	NetworkFirewall6.	NetworkFirewall6.
AWS Bonnes pratiques de sécurité fondamentales	NetworkFirewall9.	NetworkFirewall9.
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.1	Opensearch.1
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.2	Opensearch.2
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.3	Opensearch.3
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.4	Opensearch.4

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.5	Opensearch.5
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.6	Opensearch.6
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.7	Opensearch.7
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.8	Opensearch.8
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.10	Opensearch.10
AWS Bonnes pratiques de sécurité fondamentales	PCA.1	PCA.1
AWS Bonnes pratiques de sécurité fondamentales	RDS.1	RDS.1
AWS Bonnes pratiques de sécurité fondamentales	RDS.2	RDS.2
AWS Bonnes pratiques de sécurité fondamentales	RDS.3	RDS.3
AWS Bonnes pratiques de sécurité fondamentales	RDS.4	RDS.4

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	RDS.5	RDS.5
AWS Bonnes pratiques de sécurité fondamentales	RDS.6	RDS.6
AWS Bonnes pratiques de sécurité fondamentales	RDS.7	RDS.7
AWS Bonnes pratiques de sécurité fondamentales	RDS.8	RDS.8
AWS Bonnes pratiques de sécurité fondamentales	RDS.9	RDS.9
AWS Bonnes pratiques de sécurité fondamentales	RDS.10	RDS.10
AWS Bonnes pratiques de sécurité fondamentales	RDS.11	RDS.11
AWS Bonnes pratiques de sécurité fondamentales	RDS.12	RDS.12
AWS Bonnes pratiques de sécurité fondamentales	RDS.13	RDS.13
AWS Bonnes pratiques de sécurité fondamentales	RDS.14	RDS.14

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	RDS.15	RDS.15
AWS Bonnes pratiques de sécurité fondamentales	RDS.16	RDS.16
AWS Bonnes pratiques de sécurité fondamentales	RDS.17	RDS.17
AWS Bonnes pratiques de sécurité fondamentales	RDS.18	RDS.18
AWS Bonnes pratiques de sécurité fondamentales	RDS.19	RDS.19
AWS Bonnes pratiques de sécurité fondamentales	RDS.20	RDS.20
AWS Bonnes pratiques de sécurité fondamentales	RDS.21	RDS.21
AWS Bonnes pratiques de sécurité fondamentales	RDS.22	RDS.22
AWS Bonnes pratiques de sécurité fondamentales	RDS.23	RDS.23
AWS Bonnes pratiques de sécurité fondamentales	RDS.24	RDS.24

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	RDS.25	RDS.25
AWS Bonnes pratiques de sécurité fondamentales	RDS.26	RDS.26
AWS Bonnes pratiques de sécurité fondamentales	RDS.27	RDS.27
AWS Bonnes pratiques de sécurité fondamentales	RDS.34	RDS.34
AWS Bonnes pratiques de sécurité fondamentales	RDS.35	RDS.35
AWS Bonnes pratiques de sécurité fondamentales	Redshift.1	Redshift.1
AWS Bonnes pratiques de sécurité fondamentales	Redshift.2	Redshift.2
AWS Bonnes pratiques de sécurité fondamentales	Redshift.3	Redshift.3
AWS Bonnes pratiques de sécurité fondamentales	Redshift.4	Redshift.4
AWS Bonnes pratiques de sécurité fondamentales	Redshift.6	Redshift.6

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	Redshift.7	Redshift.7
AWS Bonnes pratiques de sécurité fondamentales	Redshift.8	Redshift.8
AWS Bonnes pratiques de sécurité fondamentales	Redshift.9	Redshift.9
AWS Bonnes pratiques de sécurité fondamentales	Redshift.10	Redshift.10
AWS Bonnes pratiques de sécurité fondamentales	Itinéraire 53.2	Itinéraire 53.2
AWS Bonnes pratiques de sécurité fondamentales	S3.1	S3.1
AWS Bonnes pratiques de sécurité fondamentales	S3.2	S3.2
AWS Bonnes pratiques de sécurité fondamentales	S3.3	S3.3
AWS Bonnes pratiques de sécurité fondamentales	S3.4	S3.4
AWS Bonnes pratiques de sécurité fondamentales	S3.5	S3.5

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	S3.6	S3.6
AWS Bonnes pratiques de sécurité fondamentales	S3,7	S3.7
AWS Bonnes pratiques de sécurité fondamentales	S3.8	S3.8
AWS Bonnes pratiques de sécurité fondamentales	S3.9	S3.9
AWS Bonnes pratiques de sécurité fondamentales	S3.11	S3.11
AWS Bonnes pratiques de sécurité fondamentales	S3.12	S3.12
AWS Bonnes pratiques de sécurité fondamentales	S3.13	S3.13
AWS Bonnes pratiques de sécurité fondamentales	S3,14	S3,14
AWS Bonnes pratiques de sécurité fondamentales	S3,15	S3,15
AWS Bonnes pratiques de sécurité fondamentales	S3.17	S3.17

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	S3,19	S3,19
AWS Bonnes pratiques de sécurité fondamentales	S3,19	S3,20
AWS Bonnes pratiques de sécurité fondamentales	SageMaker1.	SageMaker1.
AWS Bonnes pratiques de sécurité fondamentales	SageMaker2.	SageMaker2.
AWS Bonnes pratiques de sécurité fondamentales	SageMaker3.	SageMaker3.
AWS Bonnes pratiques de sécurité fondamentales	SecretsManager1.	SecretsManager1.
AWS Bonnes pratiques de sécurité fondamentales	SecretsManager2.	SecretsManager2.
AWS Bonnes pratiques de sécurité fondamentales	SecretsManager3.	SecretsManager3.
AWS Bonnes pratiques de sécurité fondamentales	SecretsManager4.	SecretsManager4.
AWS Bonnes pratiques de sécurité fondamentales	SNS.1	SNS.1

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	SNS.2	SNS.2
AWS Bonnes pratiques de sécurité fondamentales	SQS.1	SQS.1
AWS Bonnes pratiques de sécurité fondamentales	SSM.1	SSM.1
AWS Bonnes pratiques de sécurité fondamentales	SSM.2	SSM.2
AWS Bonnes pratiques de sécurité fondamentales	SSM.3	SSM.3
AWS Bonnes pratiques de sécurité fondamentales	SSM.4	SSM.4
AWS Bonnes pratiques de sécurité fondamentales	StepFunctions1.	StepFunctions1.
AWS Bonnes pratiques de sécurité fondamentales	WAF.1	WAF.1
AWS Bonnes pratiques de sécurité fondamentales	WAF.2	WAF.2
AWS Bonnes pratiques de sécurité fondamentales	WAF.3	WAF.3

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	WAF.4	WAF.4
AWS Bonnes pratiques de sécurité fondamentales	WAF.6	WAF.6
AWS Bonnes pratiques de sécurité fondamentales	WAF.7	WAF.7
AWS Bonnes pratiques de sécurité fondamentales	WAF.8	WAF.8
AWS Bonnes pratiques de sécurité fondamentales	WAF.10	WAF.10
AWS Bonnes pratiques de sécurité fondamentales	WAF.11	WAF.11
AWS Bonnes pratiques de sécurité fondamentales	WAF.12	WAF.12

Ressources supplémentaires

- Pour obtenir de l'aide concernant les problèmes liés à la collecte de preuves pour ce type de source de données, consultezMon évaluation ne collecte pas de preuves de contrôle de conformité auprès de AWS Security Hub.
- Pour créer un contrôle personnalisé à l'aide de ce type de source de données, consultezCréation d'un contrôle personnalisé dans AWS Audit Manager.
- Pour créer une structure personnalisée qui utilise votre contrôle personnalisé, voirCréation d'un framework personnalisé dans AWS Audit Manager.

- Pour ajouter votre contrôle personnalisé à un cadre personnalisé existant, voirModification d'un framework personnalisé dans AWS Audit Manager.

AWS Appels d'API pris en charge par AWS Audit Manager

Vous pouvez utiliser Audit Manager pour capturer des instantanés de votre AWS environnement comme preuves pour les audits. Lorsque vous créez ou modifiez un contrôle personnalisé, vous pouvez spécifier un ou plusieurs appels d' AWS API en tant que mappage de source de données pour la collecte de preuves. Audit Manager passe ensuite des appels d'API aux Services AWS personnes concernées et collecte un instantané des détails de configuration de vos AWS ressources.

Pour chaque ressource faisant l'objet d'un appel d'API, Audit Manager capture un instantané de configuration et le convertit en éléments probants. Cela se traduit par un élément probant par ressource, par opposition à un élément probant par appel d'API.

Par exemple, si l'appel d'API `ec2_DescribeRouteTables` capture des instantanés de configuration à partir de cinq tables de routage, vous obtiendrez cinq éléments probants au total pour cet appel d'API unique. Chaque élément probant est un instantané de la configuration d'une table de routage individuelle.

Rubriques

Points clés

Appels d'API paginés

Beaucoup Services AWS collectent et stockent de grandes quantités de données. Par conséquent, lorsqu'un appel d'API `list`, `describe` ou `get` tente de renvoyer vos données, les résultats peuvent être nombreux. Si la quantité de données est trop importante pour être renvoyée en une seule réponse, les résultats peuvent être divisés en éléments plus faciles à gérer grâce à la pagination. Cela divise les résultats en « pages » de données, ce qui facilite la gestion des réponses.

Certains d'entre eux Appels d'API pris en charge pour les sources de données de contrôle personnalisées sont paginés. Cela signifie qu'ils renvoient des résultats partiels dans un premier temps et nécessitent des demandes ultérieures pour renvoyer l'ensemble de résultats complet. Par exemple, l'opération DescribeDBInstances d'Amazon RDS renvoie jusqu'à 100 instances à la fois, et les demandes suivantes sont nécessaires pour renvoyer la page de résultats suivante.

Depuis le 8 mars 2023, Audit Manager prend en charge les appels d'API paginés en tant que source de données pour la collecte d'éléments probants. Auparavant, si un appel d'API paginé était utilisé comme source de données, seul un sous-ensemble de vos ressources était renvoyé dans la réponse de l'API (jusqu'à 100 résultats). Audit Manager appelle désormais l'opération d'API paginée à plusieurs reprises et obtient chaque page de résultats jusqu'à ce que toutes les ressources soient renvoyées. Pour chaque ressource, Audit Manager capture ensuite un instantané de configuration et l'enregistre comme élément probant. Étant donné que l'ensemble complet de vos ressources est désormais capturé dans la réponse de l'API, il est probable que vous remarquerez une augmentation du nombre de preuves collectées après le 8 mars 2023.

Audit Manager gère automatiquement la pagination des appels d'API pour vous. Si vous créez un contrôle personnalisé qui utilise un appel d'API paginé comme source de données, vous n'avez pas besoin de définir des paramètres de pagination.

Appels d'API pris en charge pour les sources de données de contrôle personnalisées

Dans vos contrôles personnalisés, vous pouvez utiliser l'un des appels d'API suivants comme source de données. Audit Manager peut ensuite utiliser ces appels d'API pour collecter des preuves concernant votre AWS utilisation.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
acm_ GetAccountConfiguration	Collectez un instantané des options de configuration de compte associées à votre Compte AWS.
acm_ ListCertificates	Récupérez une liste des ARN de certificat et des noms de domaine.
mise à l'échelle automatique_	Collectez un instantané des groupes Auto Scaling de votre Compte AWS.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
DescribeAutoScalingGroups	
sauvegarde_ ListBackupPlans	Récupérez la liste de tous les plans de sauvegarde actifs dans votre Compte AWS.
chambre_ GetModelInvocationLoggingConfiguration	Collectez un instantané des valeurs de configuration actuelles pour la journalisation des appels de modèles pour les modèles de votre Compte AWS.
cloudfront_ ListDistributions	Récupérez la liste de toutes les distributions de votre Compte AWS.
cloudtrail_ DescribeTrails	Collectez un instantané des paramètres d'un ou de plusieurs journaux d'activité associés à la région actuelle de votre Compte AWS.
cloudtrail_ ListTrails	Récupérez la liste des sentiers qui se trouvent dans votre Compte AWS.
cloudwatch_ DescribeAlarms	Collectez un instantané de la configuration des alarmes utilisées pour votre Compte AWS.
configuration_ DescribeConfigRules	Récupérez les détails de vos AWS Config règles.
configuration_ DescribeDeliveryChannels	Collectez un instantané de la configuration des canaux de diffusion de votre Compte AWS.
connexion directe_ DescribeDirectConnectGateways	Récupérez la liste de toutes vos AWS Direct Connect passerelles.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
connexion directe_ DescribeVirtualGateways	Récupérez la liste des passerelles privées virtuelles appartenant à votre Compte AWS.
docdb_ DescribeCertificates	Collectez une liste des certificats de votre Compte AWS.
DocDB_DescribeDBClusterParameterGroups	Collectez une liste des descriptions `DBClusterParameterGroup` de votre Compte AWS.
docdb_DescribeDBInstances	Collectez des informations sur les instances Amazon DynamoDB provisionnées de votre Compte AWS.
cloudwatch_ DescribeAlarms	Collectez des informations sur les alarmes de votre Compte AWS.
cloudtrail_ DescribeTrails	Collectez un instantané des paramètres d'un ou de plusieurs sentiers associés à votre Compte AWS.
dynamodb_ DescribeTable	Collectez des instantanés de la configuration des tables DynamoDB de votre Compte AWS. Lorsque vous utilisez cette API comme source de données, il n'est pas nécessaire de fournir le nom d'une table DynamoDB spécifique. Audit Manager utilise plutôt l'opération `ListTables` pour répertorier toutes vos tables. Pour chaque table répertoriée, Audit Manager effectue ensuite l'opération `DescribeTable` pour générer des éléments probants pour cette ressource.
dynamodb_ ListBackups	Récupérez la liste des sauvegardes DynamoDB associées à votre Compte AWS.
dynamodb_ ListTables	Récupérez une liste de l'ensemble des noms de table associés à votre Compte AWS et à votre point de terminaison actuel.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
ec2_DescribeAddresses	Collectez un instantané de vos adresses IP Elastic.
ec2_DescribeCustomerGateways	Collectez un instantané de vos passerelles clients de VPN.
ec2_DescribeEgressOnlyInternetGateways	Collectez un instantané de vos passerelles Internet de sortie uniquement.
ec2_DescribeFlowLogs	Collectez un instantané de vos journaux de flux.
ec2_DescribeInstances	Collectez un instantané de vos instances.
ec2_DescribeInternetGateways	Collectez un instantané de vos passerelles Internet.
ec2_DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	Collectez une description des associations entre les groupes d'interfaces virtuelles et les tables de routage des passerelles locales dans votre Compte AWS.
ec2_DescribeLocalGateways	Collectez un instantané de vos passerelles locales.
ec2_DescribeLocalGatewayVirtualInterfaces	Collectez un instantané de vos interfaces virtuelles de passerelle locale.
ec2_DescribeNatGateways	Collectez un instantané de vos passerelles NAT.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
ec2_ DescribeNetworkAcls	Collectez un instantané de vos ACL réseau.
ec2_ DescribeRouteTables	Collectez un instantané de vos tables de routage.
ec2_ DescribeSecurityGroups	Collectez un instantané de vos groupes de sécurité.
ec2_ DescribeSecurityGroupRules	Collectez un instantané d'une ou de plusieurs règles de votre groupe de sécurité.
ec2_ DescribeTransitGateways	Collectez un instantané de vos passerelles de transit.
ec2_ DescribeVolumes	Collectez un instantané de vos points de terminaison de VPC.
ec2_ DescribeVpcs	Collectez un instantané de vos VPC.
ec2_ DescribeVpcEndpoints	Collectez un instantané de vos points de terminaison de VPC.
ec2_ DescribeVpcEndpointConnections	Collectez un instantané des connexions des points de terminaison VPC à vos services de point de terminaison VPC, y compris les points de terminaison en attente d'acceptation.
ec2_ DescribeVpcEndpointServiceConfigurations	Collectez un instantané des configurations des services de point de terminaison VPC dans votre. Compte AWS
ec2_ DescribeVpcPeeringConnections	Collectez un instantané de vos connexions VPN.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
ec2_ DescribeVpnConnections	Collectez un instantané de vos connexions VPN.
ec2_ DescribeVpnGateways	Collectez un instantané de vos passerelles privées virtuelles.
ec2_ GetEbsDefaultKmsKeyId	Collectez un instantané du chiffrement EBS par défaut AWS KMS key pour votre Compte AWS région actuelle.
ec2_ GetEbsEncryptionByDefault	Indique si le chiffrement EBS par défaut est activé pour votre Compte AWS dans la région actuelle.
ecs_ DescribeClusters	Collectez un instantané de vos clusters ECS.
eks_ DescribeAddonVersions	Collectez un instantané des versions de vos add-on.
elasticache_ DescribeCacheClusters	Collectez un instantané de vos clusters provisionnés.
elasticache_ DescribeServiceUpdates	Collectez un instantané des mises à jour de service pour Amazon ElastiCache.
système de fichiers élastique _ DescribeAccessPoints	Collectez un instantané des points d'accès Amazon EFS de votre Compte AWS.
système de fichiers élastique_ DescribeFileSystems	Collectez un instantané de vos systèmes de fichiers Amazon EFS.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
équilibrage de charge élastique v2_ DescribeLoadBalancers	Collectez un instantané des équilibreurs de charge de votre Compte AWS.
elasticloadbalancingv2_DescribeSSLPolicies	Collectez un instantané des politiques que vous utilisez pour la négociation SSL.
équilibrage de charge élastique v2_ DescribeTargetGroups	Collectez un instantané de vos groupes cibles ELB.
elasticmapreduce_ ListSecurityConfigurations	Récupérez la liste des configurations de sécurité visibles par votre Compte AWS, ainsi que leurs noms, dates et heures de création.
événements_ ListConnections	Récupérez la liste des EventBridge connexions Amazon dans votre Compte AWS.
événements_ ListEventBuses	Récupérez la liste des bus d' EventBridge événements Amazon présents dans votre répertoire Compte AWS, y compris le bus d'événements par défaut, les bus d'événements personnalisés et les bus d'événements partenaires.
événements_ ListEventSources	Récupérez une liste des sources d'événement partenaire partagées avec votre Compte AWS.
événements_ ListRules	Récupérez la liste de vos EventBridge règles Amazon.
tuyau d'incendi_ ListDeliveryStreams	Récupérez la liste de vos flux de diffusion.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
fsx_ DescribeFileSystems	Collectez un instantané des systèmes de fichiers appartenant à votre Compte AWS.
devoir de guard_ ListDetectors	Récupérez une liste des ressources `detectorIds` pour votre GuardDuty détecteur Amazon.
iam_ GenerateCredentialReport	Générez un rapport d'informations d'identification pour votre Compte AWS.
iam_ GetAccountPasswordPolicy	Collectez un instantané de la politique de mot de passe de votre Compte AWS.
iam_ GetAccountSummary	Collectez un instantané de l'utilisation des entités et des quotas IAM dans votre Compte AWS.
iam_ ListGroups	Récupérez la liste des groupes IAM associés à un préfixe de chemin disponible dans votre. Compte AWS
Identifiant iam_ ListOpen ConnectProviders	Récupérez la liste des objets de ressource de fournisseur OpenID Connect (OIDC) IAM définis dans votre Compte AWS.
iam_ ListPolicies	Récupérez la liste de toutes les politiques gérées disponibles dans votre Compte AWS, y compris vos propres politiques gérées définies par le client et l'ensemble des politiques gérées par AWS.
iam_ ListRoles	Récupérez la liste des rôles IAM associés à un préfixe de chemin disponible dans votre. Compte AWS
iam_ListSAMLProviders	Récupérez la liste des objets de ressource de fournisseur SAML définis dans IAM de votre Compte AWS.
iam_ ListUsers	Récupérez la liste des utilisateurs IAM de votre Compte AWS.
Appareils iam_ MFA ListVirtual	Récupérez la liste des périphériques MFA virtuels définis dans votre Compte AWS.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
kafka_ ListClusters	Récupérez la liste des clusters Amazon MSK présents dans votre Compte AWS.
kafka_ ListKafka Versions	Récupérez la liste des objets de version Apache Kafka de votre Compte AWS.
kinésie_ ListStrea ms	Récupérez la liste de vos flux de données Kinesis.
kms_ GetKeyPolicy	Audit Manager utilise cette API pour collecter un instantané des stratégies de clé pour votre AWS KMS keys de votre Compte AWS. Lorsque vous utilisez cette API comme source de données, il n'est pas nécessaire de fournir le nom d'une source spécifique AWS KMS key. Audit Manager utilise plutôt l'opération `ListKeys` pour répertorier toutes vos clés KMS. Pour chaque clé KMS répertoriée, Audit Manager effectue ensuite l'opération `GetKeyPolicy` pour générer des éléments probants pour cette ressource.
kms_ GetKeyRot ationStatus	Audit Manager utilise cette API pour déterminer si la rotation automatique est activée AWS KMS keys dans votre Compte AWS. Lorsque vous utilisez cette API comme source de données, il n'est pas nécessaire de fournir le nom d'une source spécifique AWS KMS key. Audit Manager utilise plutôt l'opération `ListKeys` pour répertorier toutes vos clés KMS. Pour chaque clé KMS répertoriée, Audit Manager effectue ensuite l'opération `GetKeyRotationStatus` pour générer des éléments probants pour cette ressource.
kms_ ListKeys	Récupérez une liste des AWS KMS keys dans votre Compte AWS.
lambda_ ListFunct ions	Récupérez une liste des fonctions Lambda dans votre Compte AWS, avec la configuration spécifique à chaque version de chacune d'entre elles.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
rds_DescribeDBClusters	Collectez un instantané des clusters de base de données Amazon Aurora et des clusters de base de données multi-AZ existants dans votre Compte AWS.
rds_DescribeDBInstances	Collectez un instantané des instances RDS provisionnées de votre Compte AWS.
rds_ DescribeDbInstanceAutomatedBackups	Collectez un instantané des sauvegardes des instances actuelles et supprimées de votre Compte AWS.
rds_ DescribeDbSecurityGroups	Collectez un instantané de la base de données SecurityGroups dans votre Compte AWS.
redshift_ DescribeClusters	Collectez un instantané des clusters Amazon Redshift provisionnés de votre Compte AWS.
s3_ GetBucketEncryption	Collectez un instantané indiquant la configuration de chiffrement par défaut pour vos compartiments S3. Lorsque vous utilisez cette API comme source de données, il n'est pas nécessaire de fournir le nom d'un compartiment S3 spécifique. Audit Manager utilise plutôt l'opération `ListBuckets` pour répertorier tous vos compartiments. Pour chaque compartiment répertorié, Audit Manager effectue ensuite l'opération `GetBucketEncryption` pour générer des éléments probants pour cette ressource. Audit Manager peut uniquement fournir l'état de chiffrement pour les buckets créés en même temps Région AWS que votre évaluation. Si vous avez besoin de connaître l'état de chiffrement de tous vos compartiments S3 sur plusieurs Régions AWS, nous vous recommandons de créer une évaluation pour chacun des compartiments Région AWS où vous possédez un compartiment S3.
s3_ ListBuckets	Récupérez la liste des compartiments S3 de votre Compte AWS.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
sagemaker_ListAlgorithms	Récupérez la liste des algorithmes d'apprentissage automatique de votre Compte AWS.
sagemaker_ListDomains	Récupérez la liste des domaines de votre Compte AWS.
sagemaker_ListEndpoints	Récupérez la liste des points de terminaison de votre Compte AWS.
sagemaker_ListEndpointConfigs	Récupérez une liste des configurations de point de terminaison dans votre Compte AWS.
sagemaker_ListFlowDefinitions	Récupérez une liste des définitions de flux dans votre Compte AWS.
sagemaker_ListHumanTaskUis	Récupérez une liste des interfaces de tâches humaines de votre Compte AWS.
sagemaker_ListLabelingJobs	Récupérez la liste des tâches d'étiquetage de votre Compte AWS.
sagemaker_ListModels	Récupérez la liste des modèles de votre Compte AWS.
sagemaker_ListModelBiasJobDefinitions	Récupérez une liste des définitions de tâches liées au biais du modèle dans votre Compte AWS.
sagemaker_ListModelCards	Récupérez la liste des modèles de cartes contenus dans votre Compte AWS.
sagemaker_ListModelQualityJobDefinitions	Récupérez une liste des définitions de tâches de surveillance de la qualité des modèles dans votre Compte AWS.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
sagemaker_ ListMonitoringAlerts	Récupérez la liste des alertes pour un calendrier de surveillance donné.
sagemaker_ ListMonitoringSchedules	Récupérez une liste de tous les programmes de surveillance dans votre Compte AWS.
sagemaker_ ListTrainingJobs	Récupérez une liste des emplois de formation dans votre Compte AWS.
sagemaker_ ListUserProfiles	Récupérez une liste de profils d'utilisateurs dans votre Compte AWS.
secretsmanager_ ListSecrets	Récupérez la liste des secrets qui sont stockés dans le vôtre Compte AWS, à l'exclusion des secrets marqués pour suppression.
sns_ ListTopics	Récupérez une liste des rubriques SNS dans votre Compte AWS.
sqs_ ListQueues	Récupérez la liste des files d'attente SQS de votre. Compte AWS
waf-regional_ ListWebAcls	Récupérez la liste des objets WebACLSummary pour votre. Compte AWS
waf-regional_ ListRules	Récupérez une liste des RuleSummaryobjets pour votre Compte AWS.
waf_ ListRuleGroups	Récupérez la liste des RuleGroupSummaryobjets pour les groupes de règles de votre Compte AWS.
waf_ ListRules	Récupérez une liste des RuleSummaryobjets pour votre Compte AWS.
waf_ ListWebAcls	Récupérez la liste des objets WebACLSummary pour votre. Compte AWS

Appels d'API utilisés dans le cadre standard AWS License Manager

Dans le cadre standard AWS License Manager, Audit Manager utilise une activité personnalisée appelée `GetLicenseManagerSummary` pour collecter des éléments probants. Cette activité fait appel aux trois API du gestionnaire de licences suivantes :

- ListLicenseConfigurations
- ListAssociationsForLicenseConfiguration
- ListUsageForLicenseConfiguration

Les données renvoyées sont ensuite converties en éléments probants et jointes aux contrôles pertinents dans le cadre de votre évaluation.

Exemple

Supposons que vous utilisiez deux produits sous licence (SQL Service 2017 et Oracle Database Enterprise Edition). Tout d'abord, l'`GetLicenseManagerSummary`activité appelle l'ListLicenseConfigurationsAPI, qui fournit des détails sur les configurations de licence de votre compte. Ensuite, il ajoute des données contextuelles supplémentaires pour chaque configuration de licence en appelant ListUsageForLicenseConfigurationet ListAssociationsForLicenseConfiguration. Enfin, elle convertit les données de configuration de licence en éléments probants et les associe aux contrôles respectifs du framework (4.5 - Licence gérée par le client pour SQL Server 2017 et 3.0.4 - Licence gérée par le client pour Oracle Database Enterprise Edition).

Si vous utilisez un produit sous licence qui n'est couvert par aucun des contrôles du framework, ces données de configuration de licence sont jointes en tant qu'élément probant au contrôle suivant : 5.0 - Licence gérée par le client pour les autres licences.

Ressources supplémentaires

- Pour obtenir de l'aide concernant les problèmes liés à la collecte de preuves pour ce type de source de données, consultezMon évaluation ne collecte pas de preuves de données de configuration pour un appel d' AWS API.
- Pour créer un contrôle personnalisé à l'aide de ce type de source de données, consultezCréation d'un contrôle personnalisé dans AWS Audit Manager.
- Pour créer une structure personnalisée qui utilise votre contrôle personnalisé, voirCréation d'un framework personnalisé dans AWS Audit Manager.

- Pour ajouter votre contrôle personnalisé à un cadre personnalisé existant, voirModification d'un framework personnalisé dans AWS Audit Manager.

AWS CloudTrail noms d'événements pris en charge par AWS Audit Manager

Vous pouvez utiliser Audit Manager pour capturer les événements AWS CloudTrail de gestion et les événements de service globaux comme preuves pour les audits. Lorsque vous créez ou modifiez un contrôle personnalisé, vous pouvez spécifier un ou plusieurs noms d' CloudTrail événements sous forme de mappage de sources de données pour la collecte de preuves. Audit Manager filtre ensuite vos CloudTrail journaux en fonction des mots clés que vous avez choisis et importe les résultats sous forme de preuves de l'activité des utilisateurs.

> **Note**
>
> Audit Manager capture uniquement les événements de gestion et les événements de service mondiaux. Les événements liés aux données et les événements d'analyse ne sont pas disponibles en tant qu'éléments probants. Pour plus d'informations sur les différents types d' CloudTrail événements, consultez les CloudTrail concepts du guide de l'AWS CloudTrail utilisateur.

Par exception à ce qui précède, les CloudTrail événements suivants ne sont pas pris en charge par Audit Manager :

- kms_ GenerateDataKey
- kms_Decrypt
- sts_ AssumeRole
- kinesisvideo_ GetDataEndpoint
- kinesisvideo_ GetSignalingChannelEndpoint
- kinesisvideo_ DescribeSignalingChannel
- kinesisvideo_ DescribeStream

Depuis le 11 mai 2023, Audit Manager ne prend plus en charge les CloudTrail événements en lecture seule en tant que mots clés pour la collecte de preuves. Nous avons supprimé un total de 3 135 mots clés en lecture seule. Dans la mesure où les clients et Services AWS passent des appels en lecture aux API, les événements en lecture seule sont bruyants. Par conséquent, les mots clés en lecture seule collectent de nombreux éléments probants qui ne sont ni fiables ni pertinents pour les audits. Les mots clés en lecture seule incluent `ListDescribe`, et les appels `Get` d'API (par exemple, GetObjectet ListBucketspour Amazon S3). Si vous utilisiez l'un de ces mots clés pour recueillir des éléments probants, aucune action n'est requise. Les mots clés ont été automatiquement supprimés de la console Audit Manager et de vos évaluations, et aucun élément probant n'est collectée pour ces mots clés.

Ressources supplémentaires

- Pour obtenir de l'aide concernant les problèmes liés à la collecte de preuves pour ce type de source de données, consultezMon évaluation ne collecte pas d'éléments probants de l'activité des utilisateurs auprès d' AWS CloudTrail.
- Pour créer un contrôle personnalisé à l'aide de ce type de source de données, consultezCréation d'un contrôle personnalisé dans AWS Audit Manager.
- Pour créer une structure personnalisée qui utilise votre contrôle personnalisé, voirCréation d'un framework personnalisé dans AWS Audit Manager.
- Pour ajouter votre contrôle personnalisé à un cadre personnalisé existant, voirModification d'un framework personnalisé dans AWS Audit Manager.

Configuration AWS Audit Manager avec les paramètres recommandés

Avant de commencer à utiliser Audit Manager, il est important d'effectuer les tâches de configuration suivantes.

Ce chapitre décrit les prérequis, la configuration du compte, les autorisations utilisateur et les étapes nécessaires pour activer et configurer Audit Manager avec les fonctionnalités et intégrations recommandées. Une fois ces tâches terminées, vous serez prêt à utiliser Audit Manager et à commencer à rationaliser vos efforts d'audit et de conformité.

Table des matières

Conditions préalables à la configuration AWS Audit Manager

Avant de pouvoir l'utiliser AWS Audit Manager, vous devez vous assurer que vous avez correctement configuré vos autorisations Compte AWS et celles des utilisateurs.

Cette page décrit les étapes nécessaires pour créer un Compte AWS (si nécessaire), configurer un utilisateur administratif et accorder les autorisations requises pour accéder à Audit Manager et l'activer.

Tâches

1. Inscrivez-vous pour un Compte AWS
2. Création d'un utilisateur doté d'un accès administratif
3. Ajoutez les autorisations requises pour accéder à Audit Manager et l'activer

> **Important**
>
> Si vous êtes déjà configuré avec AWS IAM, vous pouvez ignorer les tâches 1 et 2. Cependant, vous devez effectuer la tâche 3 pour vous assurer que vous disposez des autorisations requises pour configurer Audit Manager.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.

2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, voir Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Ajoutez les autorisations requises pour accéder à Audit Manager et l'activer

Vous devez accorder aux utilisateurs les autorisations requises pour activer Audit Manager. Pour les utilisateurs qui ont besoin d'un accès complet à Audit Manager, utilisez la politique AWSAuditManagerAdministratorAccessgérée. Il s'agit d'une politique AWS gérée disponible dans votre Compte AWS environnement et recommandée aux administrateurs d'Audit Manager.

> **Tip**
>
> À titre de bonne pratique en matière de sécurité, nous vous recommandons de commencer par les politiques AWS gérées, puis de passer aux autorisations du moindre privilège. AWS les politiques gérées accordent des autorisations pour de nombreux cas d'utilisation courants. Cependant, gardez à l'esprit que, dans la mesure AWS où les politiques gérées peuvent être utilisées par tous les AWS clients, il est possible qu'elles n'accordent pas les autorisations du moindre privilège pour vos cas d'utilisation spécifiques. En conséquence, nous vous recommandons de réduire encore les autorisations en définissant des Politiques gérées par le client qui sont spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez la rubrique AWS Politiques gérées dans le AWS Identity and Access Management Guide de l'utilisateur.

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) du Guide de l'utilisateur IAM.

- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM du Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Étapes suivantes

Maintenant que vous avez configuré Compte AWS et accordé les autorisations requises, vous êtes prêt à activer Audit Manager. Pour step-by-step obtenir des instructions, voirActivant AWS Audit Manager.

Activant AWS Audit Manager

Maintenant que vous avez rempli les conditions requises pour configurer Audit Manager, vous pouvez activer le service dans votre AWS environnement.

Sur cette page, vous allez apprendre à activer Audit Manager à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager. Choisissez la méthode qui répond le mieux à vos besoins et suivez les étapes correspondantes pour que Audit Manager soit opérationnel.

Prérequis

Assurez-vous d'avoir effectué toutes les tâches décrites dansConditions préalables à la configuration AWS Audit Manager.

Procédure

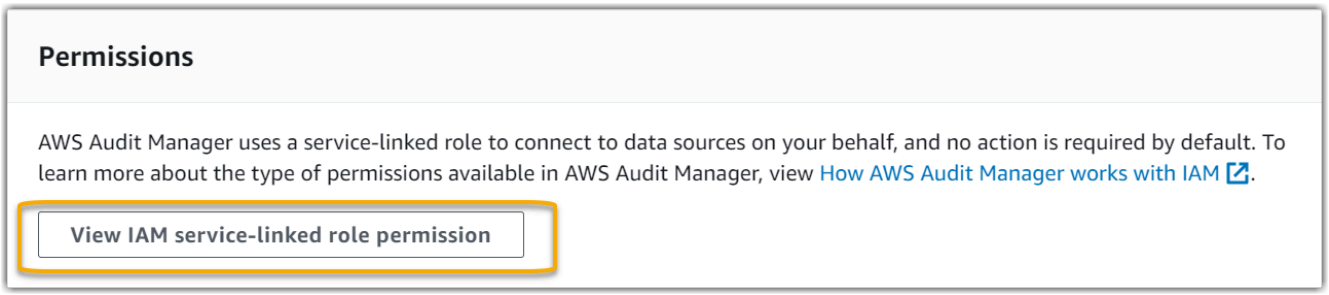
Vous pouvez activer Audit Manager à l' AWS Management Console aide de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

Audit Manager console

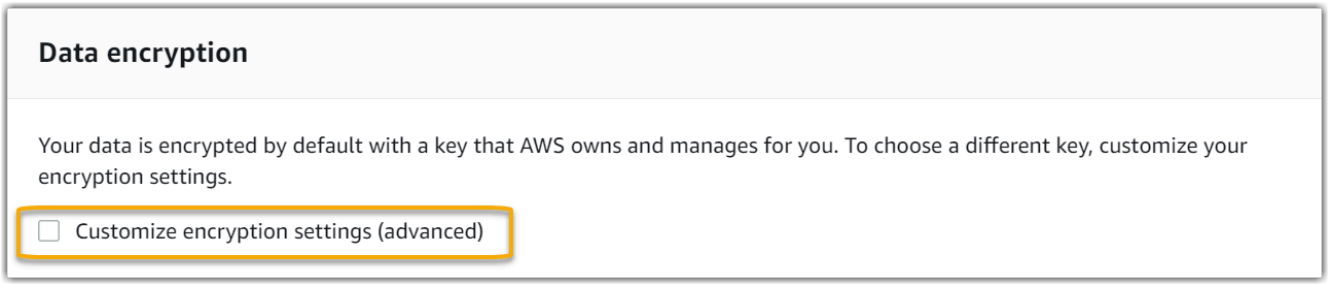
Pour activer Audit Manager à l'aide de la console

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Utilisez les informations d'identification de votre identité IAM pour vous connecter.
3. Choisissez Set up (Configurer) AWS Audit Manager.

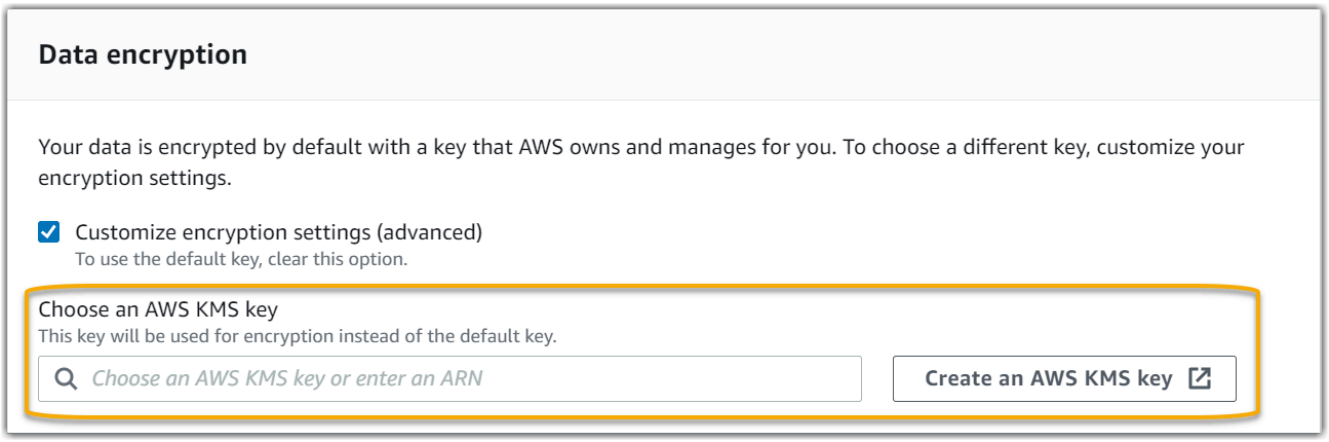
4. Sous Autorisations, aucune action n'est requise. Cela est dû au fait qu'Audit Manager utilise un rôle lié à un service pour se connecter aux sources de données en votre nom. Vous pouvez consulter le rôle lié au service en choisissant Afficher l'autorisation du rôle lié au service IAM.



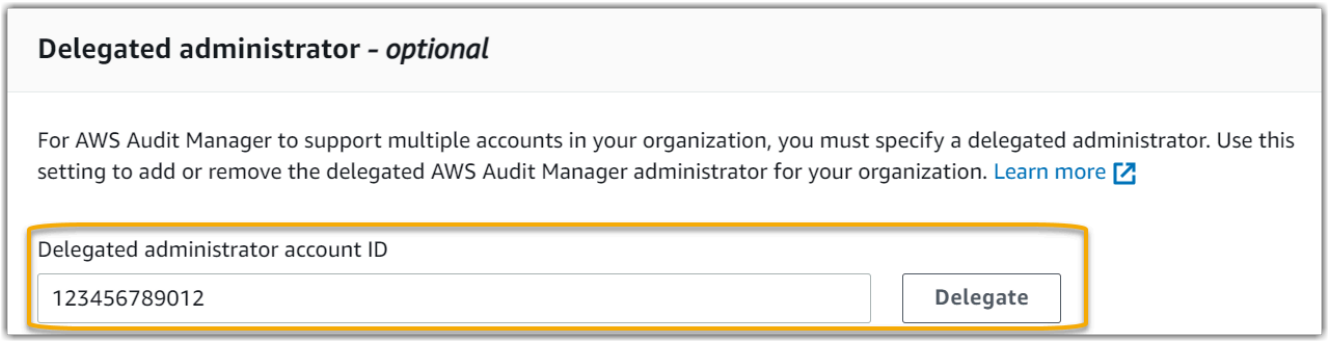
5. Sous Chiffrement des données, l'option par défaut permet à Audit Manager de créer et de gérer et AWS KMS key de stocker vos données en toute sécurité.



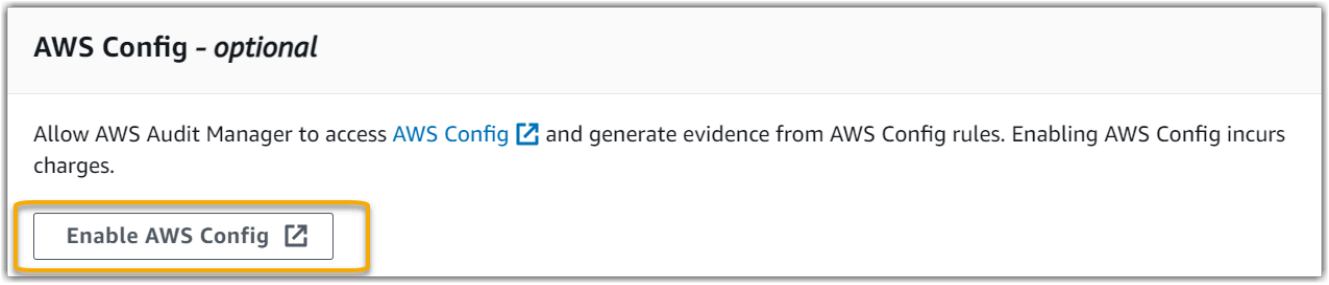
Si vous souhaitez utiliser votre propre clé gérée par le client pour chiffrer les données dans Audit Manager, cochez la case à côté de Personnaliser les paramètres de chiffrement (avancés). Choisissez alors une clé KMS existante ou créez-en une.



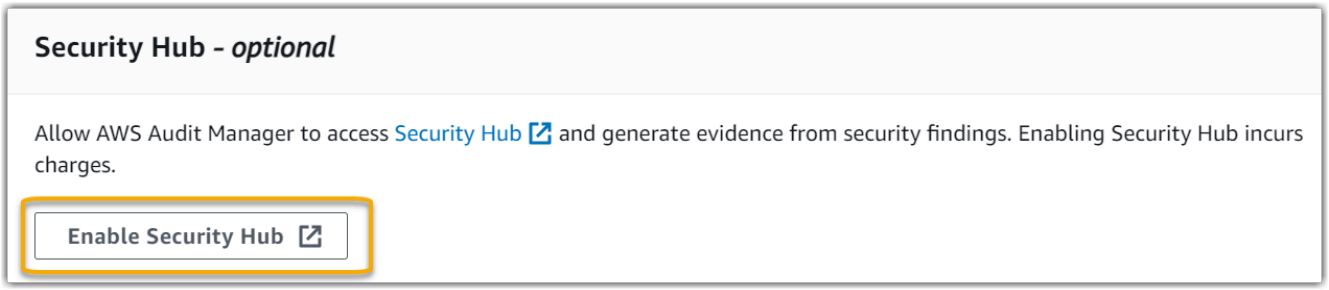
6. (Facultatif) Sous Administrateur délégué : facultatif, vous pouvez spécifier un compte d'administrateur délégué si vous souhaitez qu'Audit Manager exécute des évaluations pour plusieurs comptes. Pour plus d'informations et de recommandations, consultez Activer et configurer AWS Organizations (facultatif).



7. (Facultatif) Sous AWS Config — facultatif, nous vous recommandons de l'activer AWS Config pour une expérience optimale. Audit Manager peut alors générer des éléments probants à l'aide de AWS Config règles. Pour les instructions et les paramètres recommandés, voirActiver et configurer AWS Config (facultatif).



8. (Facultatif) Sous Security Hub – facultatif, nous vous recommandons d'activer Security Hub pour une expérience optimale. Audit Manager peut alors générer des éléments probants à l'aide des vérification Security Hub. Pour les instructions et les paramètres recommandés, voirActiver et configurer AWS Security Hub (facultatif).



9. Choisissez Compléter la configuration pour terminer le processus de configuration.

AWS CLI

Pour activer Audit Manager à l'aide du AWS CLI

Dans la ligne de commande, exécutez la commande register-account à l'aide des paramètres de configuration suivants :

- `--kms-key` (facultatif) — Utilisez ce paramètre pour chiffrer les données de votre Audit Manager à l'aide de votre propre clé gérée par le client. Si vous ne spécifiez aucune option ici, Audit Manager en crée et gère une AWS KMS key en votre nom pour le stockage sécurisé de vos données.
- `--delegated-admin-account`(facultatif) — Utilisez ce paramètre pour désigner le compte d'administrateur délégué de votre organisation pour Audit Manager. Si vous ne spécifiez aucune option ici, aucun administrateur délégué n'est enregistré.

Exemple d'entrée (remplacez *le texte de l'espace réservé* par vos propres informations) :

```
aws auditmanager register-account \
--kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
--delegated-admin-account 111122224444
```

Exemple de sortie :

```
{
    "status": "ACTIVE"
}
```

Pour plus d'informations sur les AWS CLI outils AWS CLI et pour obtenir des instructions sur leur installation, reportez-vous à ce qui suit dans le guide de AWS Command Line Interface l'utilisateur.

- Guide de l'utilisateur de l'interface de ligne de commande AWS
- Mise en place avec le AWS Command Line Interface

Audit Manager API

Pour activer Audit Manager à l'aide de l'API Audit Manager

Utilisez l'RegisterAccountopération avec les paramètres de configuration suivants :

- kmsKey (facultatif) - Utilisez ce paramètre pour chiffrer les données de votre Audit Manager à l'aide de votre propre clé gérée par le client. Si vous ne spécifiez aucune option ici, Audit Manager en crée et gère une AWS KMS key en votre nom pour le stockage sécurisé de vos données.
- delegatedAdminAccount(facultatif) — Utilisez ce paramètre pour spécifier le compte d'administrateur délégué de votre organisation pour Audit Manager. Si vous n'en spécifiez aucun, aucun administrateur délégué n'est enregistré.

Exemple d'entrée (remplacez *le texte de l'espace réservé* par vos propres informations) :

```
{
```

```
    "kmsKey":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "delegatedAdminAccount":"111122224444"
}
```

Exemple de sortie :

```
{
  "status": "ACTIVE"
}
```

Étapes suivantes

Après avoir activé Audit Manager, nous vous recommandons de configurer certaines fonctionnalités et intégrations recommandées pour une expérience optimale. Pour plus d'informations, consultez Activation des fonctionnalités recommandées et Services AWS pour AWS Audit Manager.

Activation des fonctionnalités recommandées et Services AWS pour AWS Audit Manager

Maintenant que vous l'avez activé AWS Audit Manager, il est temps de configurer les fonctionnalités et intégrations recommandées pour tirer le meilleur parti du service.

Points clés

Pour une expérience optimale dans Audit Manager, nous vous recommandons de configurer les fonctionnalités suivantes et d'activer les suivantes Services AWS.

Tâches

- Configurer les fonctionnalités recommandées d'Audit Manager
- Configurez les intégrations recommandées avec d'autres Services AWS
  - Activer et configurer AWS Config (facultatif)
  - Activer et configurer AWS Security Hub (facultatif)
  - Activer et configurer AWS Organizations (facultatif)

Configurer les fonctionnalités recommandées d'Audit Manager

Après avoir activé Audit Manager, nous vous recommandons d'activer la fonctionnalité de recherche d'éléments probants.

Outil de recherche d'éléments probants fournit un moyen puissant de rechercher des éléments probants dans Audit Manager. Au lieu de parcourir des dossiers d'éléments probants profondément imbriqués pour trouver ce que vous recherchez, vous pouvez utiliser l'outil de recherche d'éléments probants pour rechercher rapidement vos éléments probants. Si vous utilisez la recherche d'éléments probants en tant qu'administrateur délégué, vous pouvez inclure tous les comptes membres de votre organisation dans votre recherche.

Vous pouvez affiner votre requête de recherche à l'aide de filtres et de regroupements. Par exemple, si vous souhaitez obtenir une vue d'ensemble de l'état de votre système, effectuez une recherche approfondie et filtrez par évaluation, plage de dates et conformité des ressources. Si votre objectif est de remédier à une ressource spécifique, vous pouvez effectuer une recherche précise afin de cibler les éléments probants d'un contrôle ou d'un identifiant de ressource spécifique. Après avoir défini vos filtres, vous pouvez regrouper puis prévisualiser les résultats de recherche correspondants, avant de créer un rapport d'évaluation.

Configurez les intégrations recommandées avec d'autres Services AWS

Pour une expérience optimale dans Audit Manager, nous vous recommandons vivement d'activer les fonctionnalités suivantes Services AWS :

- AWS Organizations - Vous pouvez utiliser Organizations pour exécuter des évaluations d'Audit Manager sur plusieurs comptes et consolider les éléments probants dans un compte d'administrateur délégué.
- AWS Security Hubet AWS Config— Lorsque vous les activez Services AWS, ils peuvent être utilisés comme type de source de données pour les contrôles de vos évaluations Audit Manager. Audit Manager peut ensuite communiquer les résultats des contrôles de conformité directement depuis ces services.

> **Important**
>
> AWS Config Enabling, Security Hub et Organizations sont des recommandations facultatives. Toutefois, si vous activez ces services, la configuration suivante est requise.

Activer et configurer AWS Config (facultatif)

Dans Audit Manager, de nombreux contrôles sont utilisés AWS Config comme type de source de données. Pour prendre en charge ces contrôles, vous devez les activer AWS Config sur tous les comptes sur Région AWS lesquels Audit Manager est activé. Si Audit Manager essaie de collecter des preuves pour les contrôles utilisés AWS Config comme type de source de données et que les AWS Config règles associées ne sont pas activées, aucune preuve n'est collectée pour ces contrôles.

Audit Manager ne se débrouille pas AWS Config à votre place. Vous pouvez suivre ces étapes pour activer AWS Config et configurer ses paramètres.

> **Important**
>
> L'activation AWS Config est une recommandation facultative. Toutefois, si vous activez AWS Config, les paramètres suivants sont obligatoires.

Tâches à intégrer AWS Config à Audit Manager

- Étape 1 : activer AWS Config
- Étape 2 : Configurez vos AWS Config paramètres pour une utilisation avec Audit Manager

Étape 1 : activer AWS Config

Vous pouvez AWS Config l'activer à l'aide de la AWS Config console ou de l'API. Pour obtenir des instructions, consultez la section Mise en route avec AWS Config dans le AWS Config Guide du développeur.

Étape 2 : Configurez vos AWS Config paramètres pour une utilisation avec Audit Manager

Après l'activation AWS Config, assurez-vous d'activer également AWS Config les règles ou de déployer un pack de conformité pour la norme de conformité associée à votre audit. Cette étape permet à Audit Manager d'importer les résultats des règles AWS Config que vous avez activées.

Après avoir activé une AWS Config règle, nous vous recommandons de vérifier les paramètres de cette règle. Vous devez ensuite valider ces paramètres par rapport aux exigences du framework de conformité que vous avez choisi. Si nécessaire, vous pouvez mettre à jour les paramètres d'une règle

AWS Config pour vous assurer qu'elle est conforme aux exigences du framework. Vous pouvez ainsi garantir que vos évaluations collectent les éléments probants de contrôle de conformité corrects pour un framework donné.

Supposons, par exemple, que vous créez une évaluation pour CIS v1.2.0. Ce framework comporte un contrôle nommé 1.4 — Assurez-vous que les clés d'accès sont renouvelées tous les 90 jours ou moins. Dans AWS Config, la access-keys-rotatedrègle comporte un `maxAccessKeyAge` paramètre dont la valeur par défaut est de 90 jours. Par conséquent, la règle s'aligne sur les exigences de contrôle. Si vous n'utilisez pas la valeur par défaut, assurez-vous qu'elle est égale ou supérieure à l'exigence de 90 jours de CIS v1.2.0.

Vous trouverez les détails des paramètres par défaut pour chaque règle gérée dans la documentation AWS Config. Pour obtenir des instructions sur la configuration d'une règle, consultez la section Utilisation des règles AWS Config gérées.

Activer et configurer AWS Security Hub (facultatif)

Dans Audit Manager, de nombreux contrôles utilisent Security Hub comme type de source de données. Pour prendre en charge ces contrôles, vous devez les activer Security Hub sur tous les comptes sur chaque région où Audit Manager est activé. Si Audit Manager essaie de collecter des éléments probants pour les contrôles utilisant Security Hub comme type de source de données et que les règles Security Hub associées ne sont pas activées, aucun élément probant n'est collecté pour ces contrôles.

Audit Manager ne gère pas Security Hub à votre place. Vous pouvez suivre ces étapes pour activer Security Hub et configurer ses paramètres.

> **Important**
>
> L'activation de Security Hub est une recommandation facultative. Toutefois, si vous activez Security Hub, les paramètres suivants sont obligatoires.

Tâches à intégrer AWS Security Hub à Audit Manager

- Étape 1 : activer AWS Security Hub
- Étape 2 : configurer vos paramètres Security Hub pour une utilisation avec Audit Manager
- Étape 3 : Configuration des paramètres des organisations pour votre organisation

Étape 1 : activer AWS Security Hub

Vous pouvez activer Security Hub à l'aide de la console ou de l'API. Pour obtenir des instructions, consultez Configuration AWS Security Hub dans le guide de l'utilisateur AWS Security Hub .

Étape 2 : configurer vos paramètres Security Hub pour une utilisation avec Audit Manager

Après avoir activé Security Hub, assurez-vous d'effectuer également les opérations suivantes :

- Activer AWS Config et configurer l'enregistrement des ressources : Security Hub utilise des AWS Config règles liées aux services pour effectuer la plupart de ses contrôles de sécurité. Pour prendre en charge ces contrôles, ils AWS Config doivent être activés et configurés pour enregistrer les ressources requises pour les contrôles que vous avez activés dans chaque norme activée.
- Activer toutes les normes de sécurité : cette étape permet à Audit Manager d'importer les résultats pour toutes les normes de conformité prises en charge.
- Activez le paramètre des résultats de contrôle consolidés dans Security Hub.- Ce paramètre est activé par défaut si vous activez Security Hub le 23 février 2023 ou après cette date.

> **Note**
>
> Lorsque vous activez les résultats consolidés, Security Hub produit un résultat unique pour chaque contrôle de sécurité (même lorsque le même contrôle est utilisé pour plusieurs normes). Chaque résultat du Security Hub est collecté dans le cadre d'une évaluation de ressource unique dans Audit Manager. Par conséquent, les résultats consolidés se traduisent par une diminution du nombre total d'évaluations uniques des ressources effectuées par Audit Manager pour les résultats de Security Hub. Pour cette raison, l'utilisation de résultats consolidés peut souvent entraîner une réduction des coûts d'utilisation de votre Audit Manager. Pour plus d'informations sur l'utilisation de Security Hub comme type de source de données, consultez AWS Security Hub commandes prises en charge par AWS Audit Manager. Pour plus d'informations sur la tarification d'Audit Manager, consultez AWS Audit Manager Tarification.

Étape 3 : Configuration des paramètres des organisations pour votre organisation

Si vous utilisez AWS Organizations et souhaitez collecter des preuves Security Hub à partir de vos comptes membres, vous devez également suivre les étapes suivantes dans Security Hub.

Pour configurer les paramètres Security Hub de votre organisation

1. Connectez-vous à la AWS Security Hub console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/securityhub/.
2. À l'aide AWS Organizations de votre compte de gestion, désignez un compte en tant qu'administrateur délégué pour Security Hub. Pour plus d'informations, consultez Désignation d'un compte administrateur Security Hub dans le Guide de l'utilisateur AWS Security Hub .

   > **Note**
   >
   > Vérifiez que le compte d'administrateur délégué que vous utilisez dans Security Hub est le même que celui que vous utilisez dans Audit Manager.

3. À l'aide de votre compte d'administrateur délégué d'organisations, allez dans Paramètres, Comptes, sélectionnez tous les comptes, puis ajoutez-les en tant que membres en sélectionnant Inscription automatique. Pour plus d'informations, consultez la rubrique Activation de comptes membre de votre organisation du Guide de l'utilisateur AWS Security Hub .
4. Activez AWS Config cette option pour chaque compte membre de l'organisation. Pour plus d'informations, consultez la rubrique Activation de comptes membre de votre organisation du Guide de l'utilisateur AWS Security Hub .
5. Activez la norme de sécurité PCI DSS pour chaque compte membre de l'organisation. La norme AWS CIS Foundations Benchmark et la norme AWS Foundational Best Practices sont déjà activées par défaut. Pour plus d'informations, consultez la rubrique Activation d'une norme de sécurité dans le AWS Security Hub Guide de l'utilisateur.

Activer et configurer AWS Organizations (facultatif)

Audit Manager prend en charge plusieurs comptes via l'intégration avec AWS Organizations. Audit Manager peur exécuter des évaluations sur plusieurs comptes et consolider les éléments probants dans un compte d'administrateur délégué. L'administrateur délégué dispose des autorisations nécessaires pour créer et gérer des ressources Audit Manager avec l'organisation comme zone de confiance. Seul le compte de gestion peut désigner un administrateur délégué.

> **Important**
>
> L'activation AWS Organizations est une recommandation facultative. Toutefois, si vous l'activez AWS Organizations, les paramètres suivants sont obligatoires.

Tâches à intégrer AWS Organizations à Audit Manager

- Étape 1 : créer une organisation ou y adhérer
- Étape 2 : activer toutes les fonctionnalités de votre organisation
- Étape 3 : spécifier un administrateur délégué pour Audit Manager

Étape 1 : créer une organisation ou y adhérer

Si vous Compte AWS ne faites pas partie d'une organisation, vous pouvez créer ou rejoindre une organisation. Pour obtenir des instructions pratiques, veuillez consulter Création et gestion d'une organisation dans le Guide de l'utilisateur AWS Organizations .

Étape 2 : activer toutes les fonctionnalités de votre organisation

Vous devez ensuite activer toutes les fonctionnalités de votre organisation. Pour obtenir les instructions, consultez Activation de toutes les fonctionnalités de votre organisation dans le Guide de l'utilisateur AWS Organizations .

Étape 3 : spécifier un administrateur délégué pour Audit Manager

Nous vous recommandons d'activer Audit Manager à l'aide d'un compte de gestion des organisations puis de spécifier un administrateur délégué. Ensuite, vous pouvez utiliser le compte d'administrateur délégué pour vous connecter et exécuter des évaluations. À titre de bonne pratique, nous vous recommandons de créer uniquement des évaluations à l'aide du compte administrateur délégué plutôt que du compte de gestion.

Pour ajouter ou modifier un administrateur délégué après avoir activé Audit Manager, consultez Ajouter un administrateur délégué etModification d'un administrateur délégué.

Étapes suivantes

Maintenant que vous avez configuré Audit Manager avec les paramètres recommandés, vous êtes prêt à commencer à utiliser le service.

- Pour commencer votre première évaluation, consultezTutoriel pour les responsables d'audit : création d'une évaluation.
- Pour mettre à jour vos paramètres à l'avenir, consultezRévision et configuration de vos AWS Audit Manager paramètres.

Commencer avec AWS Audit Manager

Utilisez les step-by-step didacticiels de cette section pour apprendre à effectuer des tâches à l'aide de AWS Audit Manager.

Tip

Les tutoriels suivants sont classés par public. Choisissez le tutoriel qui vous convient en fonction de votre rôle en tant que responsable de l'audit ou délégué.

- Les responsables de l'audit sont des utilisateurs d'Audit Manager chargés de créer et de gérer les évaluations. Dans le monde des affaires, les responsables de l'audit sont généralement des professionnels de la gouvernance, de la gestion des risques et de la conformité (GRC). Dans le contexte d'Audit Manager, toutefois, des personnes SecOps ou des DevOps équipes peuvent également assumer la personnalité d'un responsable de l'audit. Les responsables de l'audit peuvent demander l'assistance d'un expert en la matière, également appelé délégué, pour vérifier des contrôles spécifiques et valider les éléments probants. Les responsables de l'audit doivent posséder les autorisations nécessaires pour gérer une évaluation.
- Les délégués sont des experts en la matière dotés d'une expertise technique ou commerciale spécialisée. Bien qu'ils ne possèdent ni ne gèrent les évaluations d'Audit Manager, ils peuvent tout de même y contribuer. Les délégués aident les responsables de l'audit dans des tâches telles que la validation des éléments probants relatifs aux contrôles relevant de leur domaine d'expertise. Les délégués disposent d'autorisations limitées dans Audit Manager. La raison en est que les responsables de l'audit délèguent des ensembles de contrôles spécifiques pour vérification, et non des évaluations complètes.

Pour plus d'informations sur ces personnages et les autres concepts d'Audit Manager, consultez audit owner et delegate dans la Comprendre AWS Audit Manager les concepts et la terminologie section de ce guide.
Pour plus d'informations sur les autorisations IAM recommandées pour chaque persona, consultez Politiques recommandées pour les personas utilisateurs dans AWS Audit Manager.

Tutoriels Audit Manager

Création d'une évaluation

Public cible : Responsables de l'audit

Vue d'ensemble : suivez step-by-step les instructions pour créer votre première évaluation et être rapidement opérationnel. Ce didacticiel explique comment utiliser un cadre standard pour créer une évaluation et commencer la collecte automatisée de preuves.

Vérification d'un ensemble de contrôles

Public : Délégués

Vue d'ensemble : aidez le responsable de l'audit en vérifiant les éléments probants relatifs aux contrôles relevant de votre domaine d'expertise. Apprenez à examiner les ensembles de contrôles et les preuves associées, à ajouter des commentaires, à télécharger des preuves et à mettre à jour le statut d'un contrôle.

Tutoriel pour les responsables d'audit : création d'une évaluation

Ce didacticiel fournit une introduction à AWS Audit Manager. Dans ce didacticiel, vous allez créer une évaluation à l'aide duAWS Audit Manager Exemple de cadre. En créant une évaluation, vous lancez le processus continu de collecte automatisée d'éléments probants pour les contrôles dans ce framework.

> **Note**
>
> AWS Audit Manager aide à recueillir des preuves pertinentes pour vérifier le respect de cadres de conformité et de réglementations spécifiques. Cependant, il n'évalue pas votre conformité lui-même. Les preuves collectées par ce biais peuvent AWS Audit Manager donc ne pas inclure toutes les informations sur votre AWS utilisation nécessaires aux audits. AWS Audit Manager ne remplace pas un conseiller juridique ou un expert en conformité.

Prérequis

Avant de commencer ce didacticiel, assurez-vous de remplir les conditions suivantes :

- Vous avez rempli tous les prérequis décrits dans Configuration AWS Audit Manager avec les paramètres recommandés. Vous devez utiliser votre console Compte AWS et la AWS Audit Manager console pour terminer ce didacticiel.
- Votre identité IAM est dotée des autorisations appropriées pour créer et gérer une évaluation dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont Permettre aux utilisateurs un accès administrateur complet à AWS Audit Manager etAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.
- Vous connaissez la terminologie et les fonctionnalités d'Audit Manager. Pour une présentation générale, consultez Qu'est-ce que c'est AWS Audit Manager ? et Comprendre AWS Audit Manager les concepts et la terminologie.

Procédure

Tâches

- Étape 1 : Indiquer les détails de l'évaluation
- Étape 2 : Spécifier le champ Comptes AWS d'application
- Étape 3 : Spécifier les responsables de l'audit
- Étape 4 : vérifier et créer

Étape 1 : Indiquer les détails de l'évaluation

Pour la première étape, sélectionnez un framework et fournissez des informations de base pour votre évaluation.

Pour indiquer les détails de l'évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Choisissez Lancer AWS Audit Manager.
3. Dans le bandeau vert en haut de l'écran, choisissez Commencer avec un framework.

4. Choisissez le framework de votre choix, puis choisissez Créer une évaluation à partir du framework. Pour ce didacticiel, utilisez le AWS Audit Manager Sample Framework.
5. Sous Nom de l'évaluation, saisissez un nom pour votre évaluation.
6. (Facultatif) Sous Description de l'évaluation, saisissez une description pour votre évaluation.
7. Sous Destination des rapports d'évaluation, choisissez le compartiment S3 dans lequel vous souhaitez enregistrer vos rapports d'évaluation.
8. Sous Frameworks, vérifiez que AWS Audit Manager Sample Framework est sélectionné.
9. (Facultatif) Sous Balises, choisissez Ajouter une nouvelle étiquette pour associer une balise à votre évaluation. Vous pouvez indiquer une clé et une valeur pour chaque balise. La clé de balise est obligatoire et peut être utilisée comme critère de recherche lorsque vous recherchez cette évaluation.
10. Choisissez Suivant.

Étape 2 : Spécifier le champ Comptes AWS d'application

Spécifiez ensuite les AWS comptes que vous souhaitez inclure dans le champ de votre évaluation.

AWS Audit Manager s'intègre à AWS Organizations, afin que vous puissiez exécuter une évaluation Audit Manager sur plusieurs comptes et consolider les preuves dans un compte d'administrateur délégué. Pour activer Organizations dans Audit Manager (si ce n'est pas déjà fait), consultez Activer et configurer AWS Organizations (facultatif) sur la page Configuration de ce guide.

> **Note**
>
> Audit Manager peut prendre en charge jusqu'à 200 comptes dans le cadre d'une évaluation. Si vous essayez d'inclure plus de 200 comptes, la création de l'évaluation risque d'échouer.

Pour indiquer les comptes concernés

1. Sous Comptes AWS, sélectionnez les éléments Comptes AWS que vous souhaitez inclure dans le champ de votre évaluation.
   - Si vous avez activé Organizations dans Audit Manager, plusieurs comptes sont répertoriés.
   - Si vous n'avez pas activé Organizations dans Audit Manager, seul votre compte actuel est répertorié.
2. Choisissez Suivant.

Étape 3 : Spécifier les responsables de l'audit

Dans cette étape, vous indiquez les responsables de l'audit pour votre évaluation. Les responsables de l'audit sont les personnes de votre lieu de travail, généralement issues de la GRC ou d' DevOps équipes SecOps, qui sont chargées de gérer l'évaluation de l'Audit Manager. Nous leur recommandons d'utiliser cette AWSAuditManagerAdministratorAccesspolitique.

Pour indiquer les responsables de l'audit

1. Sous Responsables de l'audit, choisissez les responsables de l'audit pour votre évaluation. Pour trouver d'autres responsables d'audit, utilisez la barre de recherche pour effectuer une recherche par nom ou Compte AWS.
2. Choisissez Suivant.

Étape 4 : vérifier et créer

Vérifiez les informations de votre évaluation. Pour modifier les informations d'une étape, choisissez Modifier. Lorsque vous avez terminé, choisissez Créer une évaluation pour commencer la collecte continue de preuves.

Une fois que vous avez créé une évaluation, la collecte d'éléments probants se poursuit jusqu'à ce que vous passiez le statut de l'évaluation à inactif. Vous pouvez également arrêter la collecte d'éléments probants pour un contrôle précis en faisant passer le statut du contrôle à inactif.

> **Note**
>
> Les preuves automatisées sont disponibles 24 heures après la création de l'évaluation. Audit Manager collecte automatiquement des éléments probants à partir de plusieurs sources de données, et la fréquence de cette collecte d'éléments probants est basée sur le type d'éléments probants. Pour plus d'informations, consultez Fréquence de collecte des éléments probants dans ce guide.

Ressources supplémentaires

Nous vous recommandons de continuer à vous renseigner sur les concepts et les outils présentés dans ce didacticiel. Pour ce faire, consultez les ressources suivantes :

- Consulter les détails de l'évaluation dans AWS Audit Manager— Vous présente la page des détails de l'évaluation où vous pouvez explorer les différents éléments de votre évaluation.
- Gestion des évaluations dans AWS Audit Manager — S'appuie sur ce tutoriel et fournit des informations approfondies sur les concepts et les tâches de gestion d'une évaluation. Dans ce chapitre, nous vous recommandons particulièrement de consulter les rubriques suivantes :
  - Comment créer une évaluation à partir d'un autre framework
  - Comment vérifier les éléments probants d'une évaluation et générer un rapport d'évaluation
  - Comment modifier le statut d'une évaluation ou supprimer une évaluation
- Utilisation de la bibliothèque de frameworks pour gérer les frameworks dans AWS Audit Manager — Présente la bibliothèque de cadres et explique comment créer un framework personnalisé pour vos propres besoins de conformité spécifiques.
- Utilisation de la bibliothèque de commandes pour gérer les commandes dans AWS Audit Manager—Présente la bibliothèque de contrôles et explique comment créer un contrôle personnalisé à utiliser dans votre framework personnalisé.
- Comprendre AWS Audit Manager les concepts et la terminologie — Fournit les définitions des concepts et de la terminologie utilisés dans Audit Manager.
- [Vidéo] Collectez des preuves et gérez les données d'audit à l'aide de AWS Audit Manager : montre le processus de création d'une évaluation décrit dans ce didacticiel, ainsi que d'autres tâches telles que la révision d'un contrôle et la génération d'un rapport d'évaluation.

Tutoriel pour les délégués : Vérification d'un ensemble de contrôles

Ce tutoriel explique comment vérifier un ensemble de contrôles qui a été partagé avec vous par un responsable d'audit dans AWS Audit Manager.

Les responsables de l'audit utilisent Audit Manager pour créer des évaluations et collecter des preuves des contrôles effectués dans le cadre de cette évaluation. Les responsables d'audit peuvent parfois avoir des questions ou besoin d'aide pour valider les éléments probants d'une série de contrôles. Dans ce cas, le responsable de l'audit peut déléguer un ensemble de contrôles à un expert en la matière pour vérification.

En tant que délégué, vous aidez les responsables de l'audit à vérifier les éléments probants collectés pour les contrôles relevant de votre domaine d'expertise.

Prérequis

Avant de commencer ce tutoriel, vérifiez d'abord que vous remplissez les conditions suivantes :

- Compte AWS Le vôtre est configuré. Pour terminer ce didacticiel, vous devez utiliser à la fois votre console Compte AWS et la console Audit Manager. Pour plus d'informations, consultez Configuration AWS Audit Manager avec les paramètres recommandés.
- Vous connaissez la terminologie et les fonctionnalités d'Audit Manager. Pour une présentation générale d'Audit Manager, reportez-vous aux sections Qu'est-ce que c'est AWS Audit Manager ? et Comprendre AWS Audit Manager les concepts et la terminologie.

Procédure

Tâches

Étape 1 : passez en revue vos notifications

Commencez par vous connecter à Audit Manager où vous pouvez accéder à vos notifications pour voir les ensembles de contrôle qui vous ont été délégués pour examen.

Pour consulter vos notifications

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation de gauche, choisissez Notifications.
3. Sur la page Notifications, vous pouvez consulter la liste des ensembles de contrôles qui vous ont été délégués. Les tableaux de notifications comprennent les informations suivantes :

Name (Nom)	Description
Date	Date à laquelle l'ensemble de contrôle a été délégué.
Évaluation	Nom de l'évaluation associée à l'ensemble de contrôles. Vous pouvez choisir un nom d'évaluation pour ouvrir la page détaillée de l'évaluation.
Kit de commande	Le nom de l'ensemble de contrôles qui vous a été délégué pour révision.
Source	L'utilisateur ou le rôle qui vous a délégué le jeu de contrôle.
Description	Les instructions de révision fournies par le responsable de l'audit.

> **Tip**
>
> Vous pouvez également vous abonner à une rubrique SNS pour recevoir des alertes par e-mail lorsqu'un ensemble de contrôles vous est attribué pour vérification. Pour plus d'informations, consultez Notifications dans AWS Audit Manager.

Étape 2 : Vérifier l'ensemble de contrôles et les éléments probants connexes

L'étape suivante consiste à vérifier les ensembles de contrôles que le responsable de l'audit vous a délégués. En examinant les contrôles et leurs éléments probants, vous pouvez déterminer si une action supplémentaire est nécessaire pour un contrôle. Les actions supplémentaires peuvent inclure le téléchargement manuel de preuves supplémentaires pour démontrer la conformité, ou le dépôt d'un commentaire à propos de ce contrôle.

Pour vérifier un ensemble de contrôles

1. À partir de la page Notifications, vérifiez la liste des ensembles de contrôles qui vous ont été délégués. Identifiez ensuite celui que vous souhaitez vérifier et choisissez le nom de l'évaluation correspondante.

2. Sous l'onglet Contrôles de la page détaillée de l'évaluation, faites défiler la page vers le bas jusqu'au tableau Séries de contrôles.
3. Dans la colonne Contrôles regroupés par séries de contrôles, cliquez sur le nom d'une série de contrôles pour en afficher le détail. Puis, sélectionnez le nom d'un contrôle pour ouvrir sa page détaillée.
4. (Facultatif) Choisissez Mettre à jour le statut du contrôle pour modifier le statut du contrôle. Pendant que votre révision est en cours, vous pouvez marquer le statut comme En cours de révision.
5. Consultez les informations relatives au contrôle dans les dossiers Preuves, Détails, Sources de preuves, Commentaires et Changelog. Pour en savoir plus sur chacun de ces onglets et sur la façon de comprendre les données qu'ils contiennent, consultezRévision d'un contrôle d'évaluation dans AWS Audit Manager.

Pour vérifier les éléments probants d'un contrôle

1. Sur la page détaillée du contrôle, choisissez l'onglet Dossiers d'éléments probants.
2. Accédez au tableau Dossiers d'éléments probants, où la liste des dossiers contenant les éléments probants de ce contrôle est affichée. Ces dossiers sont organisés et nommés en fonction de la date à laquelle les éléments probants contenus dans ce dossier ont été collectés.
3. Sélectionnez le nom d'un dossier d'éléments probants pour l'ouvrir. À partir de là, vous pouvez consulter un résumé de tous les éléments probants recueillis à cette date. Pour comprendre ces informations, consultezRévision d'un dossier de preuves dans AWS Audit Manager.
4. À partir de la page récapitulative du dossier d'éléments probants, accédez au tableau Éléments probants. Dans la colonne Heure, choisissez une rubrique pour ouvrir et vérifier les détails des éléments probants recueillis à ce moment-là. Pour comprendre ces informations, consultezExamen des preuves dans AWS Audit Manager.

Étape 3. Ajouter des preuves manuelles (facultatif)

Bien qu'il collecte AWS Audit Manager automatiquement des preuves pour de nombreux contrôles, dans certains cas, vous devrez peut-être fournir des preuves supplémentaires. Dans ces cas, vous pouvez ajouter manuellement vos propres preuves qui vous aideront à démontrer le respect de ce contrôle.

Pour ajouter des preuves manuelles à un contrôle

Il existe plusieurs méthodes pour ajouter des preuves manuelles à un contrôle. Vous pouvez importer un fichier depuis Amazon S3, charger un fichier depuis votre navigateur ou saisir une réponse textuelle. Pour les instructions relatives à chaque méthode, voirAjouter des preuves manuelles dans AWS Audit Manager.

Étape 4 : Ajouter un commentaire pour un contrôle (facultatif)

Vous pouvez ajouter des commentaires pour tous les contrôles que vous vérifiez. Ces commentaires sont visibles par le responsable de l'audit. Par exemple, vous pouvez laisser un commentaire pour fournir une mise à jour du statut et confirmer que vous avez résolu tout problème lié à ce contrôle.

Pour ajouter un commentaire à un contrôle

1. À partir de la page Notifications, vérifiez la liste des ensembles de contrôles qui vous ont été délégués. Recherchez l'ensemble de contrôles pour lequel vous souhaitez laisser un commentaire, puis choisissez le nom de l'évaluation associée.
2. Choisissez l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'à Ensembles de contrôles, puis sélectionnez le nom d'un contrôle pour l'ouvrir.
3. Sélectionnez l'onglet Commentaires.
4. Sous Envoyer des commentaires, saisissez votre commentaire dans la zone de texte.
5. Choisissez Soumettre les commentaires pour ajouter votre commentaire. Votre commentaire apparaît désormais dans la section Commentaires précédents de la page, avec tout autre commentaire concernant ce contrôle.

Étape 5 : Marquer un contrôle comme vérifié (facultatif)

La modification du statut d'un contrôle est facultative. Cependant, nous vous recommandons de modifier le statut de chaque contrôle sur Vérifié au fur et à mesure de votre vérification de ce contrôle. Quel que soit le statut de chaque contrôle individuel, vous pouvez toujours soumettre les contrôles au responsable de l'audit.

Pour marquer un contrôle comme vérifié

1. À partir de la page Notifications, vérifiez la liste des ensembles de contrôles qui vous ont été délégués. Recherchez le jeu de contrôles qui contient le contrôle que vous souhaitez marquer comme vérifié. Choisissez ensuite le nom de l'évaluation associée pour ouvrir la page détaillée de l'évaluation.

2. Sous l'onglet Contrôles de la page détaillée de l'évaluation, faites défiler la page vers le bas jusqu'au tableau Séries de contrôles.
3. Dans la colonne Contrôles regroupés par séries de contrôles, cliquez sur le nom d'une série de contrôles pour en afficher le détail. Choisissez le nom d'un contrôle pour ouvrir la page détaillée du contrôle.
4. Choisissez Mettre à jour le statut du contrôle et remplacez le statut par Vérifié.
5. Dans la fenêtre contextuelle qui apparaît, choisissez Mettre à jour le statut du contrôle pour confirmer que vous avez terminé de vérifier le contrôle.

Étape 6. Soumettre l'ensemble de contrôle vérifié au responsable de l'audit

Lorsque vous avez terminé de vérifier de tous les contrôles, soumettez-les à nouveau au responsable de l'audit pour lui faire savoir que vous avez terminé votre vérification.

Pour soumettre un ensemble de contrôle vérifié au responsable de l'audit

1. Sur la page Notifications, vérifiez la liste des ensembles de contrôles qui vous ont été assignés. Recherchez l'ensemble de contrôles que vous souhaitez soumettre au responsable de l'audit, puis choisissez le nom de l'évaluation associée.
2. Faites défiler la page jusqu'au tableau Ensembles de contrôles, sélectionnez l'ensemble de contrôles que vous souhaitez renvoyer au responsable de l'audit, puis choisissez Soumettre pour vérification.
3. Dans la fenêtre contextuelle qui apparaît, vous pouvez ajouter des commentaires généraux sur cet ensemble de contrôles avant de choisir Soumettre pour vérification.

Une fois que vous avez soumis le contrôle au responsable de l'audit, celui-ci peut consulter les commentaires que vous lui avez laissés.

Ressources supplémentaires

Vous pouvez continuer à en apprendre davantage sur les concepts présentés dans ce tutoriel. Voici quelques ressources recommandées :

- Consulter les détails de l'évaluation dans AWS Audit Manager- Vous présente la page de détails de l'évaluation, où vous pouvez explorer les différents composants d'une évaluation d'Audit Manager.

- Révision d'un contrôle d'évaluation dans AWS Audit Manageret Examen des preuves dans AWS Audit Manager - Fournit des définitions pour vous aider à comprendre les contrôles et les preuves d'une évaluation.
- Comprendre AWS Audit Manager les concepts et la terminologie : fournit les définitions des concepts et de la terminologie utilisés dans Audit Manager.

Utilisation du tableau de bord d'Audit Manager

Avec le tableau de bord d'Audit Manager, vous pouvez visualiser les éléments probants non conformes dans vos évaluations actives. C'est un moyen pratique et rapide de suivre vos évaluations, de rester informé et de résoudre les problèmes de manière proactive. Par défaut, le tableau de bord fournit une vue agrégée de haut en bas de toutes vos évaluations actives. Grâce à cette vue, vous pouvez identifier visuellement les problèmes liés à vos évaluations sans avoir à passer au crible de grandes quantités d'élément probants individuels.

Le tableau de bord est le premier écran que vous voyez lorsque vous vous connectez à la console Audit Manager. Il contient deux widgets qui affichent les données et les indicateurs de performance clés (KPI) les plus pertinents pour vous. À l'aide d'un filtre d'évaluation, vous pouvez affiner ces données afin de vous concentrer sur les KPI d'une évaluation spécifique. À partir de là, vous pouvez passer en revue les groupements de domaines de contrôle afin d'identifier les contrôles présentant le plus d'éléments probants non conformes. Vous pouvez ensuite explorer les contrôles sous-jacents pour examiner et résoudre les problèmes.

> **Note**
>
> Si vous utilisez Audit Manager pour la première fois ou si aucune évaluation n'est active, aucune donnée n'est affichée dans le tableau de bord. Pour commencer, créez une évaluation. Cette étape marque le début de la collecte continue d'éléments probants. Après une période de 24 heures, les données d'éléments probants agrégées commenceront à apparaître dans le tableau de bord. Vous pouvez lire les sections suivantes pour savoir comment comprendre et interpréter ces données.

Cette page couvre les rubriques suivantes :

Rubriques

Concepts et terminologie du tableau de bord

Cette section couvre les informations importantes à connaître sur le tableau de bord d'Audit Manager avant de commencer à l'utiliser.

Autorisations et visibilité

Les responsables de l'audit et les délégués ont accès au tableau de bord. Cela signifie que ces deux personnes peuvent voir les statistiques et les agrégats de toutes les évaluations actives de votre. Compte AWS L'accès aux mêmes informations permet à toute votre équipe de se concentrer sur les mêmes KPI et objectifs.

Filtres

Audit Manager fournit un niveau de page the section called "Filtre d'évaluation" que vous pouvez appliquer à tous les widgets de votre tableau de bord.

Éléments probants non conformes

Le tableau de bord met en évidence les contrôles de vos évaluations qui contiennent des éléments probants de vérification de conformité et une conclusion de non-conformité. Les preuves du contrôle de conformité concernent les contrôles qui utilisent AWS Config ou AWS Security Hub en tant que type de source de données. Pour ce type d'élément probant, Audit Manager rapporte le résultat d'un contrôle de conformité directement depuis ces services. Si Security Hub indique un résultat d'échec ou AWS Config un résultat non conforme, Audit Manager classe les éléments probants comme non conformes.

Éléments probants non concluants

Les éléments probants ne sont pas concluants si un contrôle de conformité n'est pas disponible ou applicable. Par conséquent, aucune évaluation de conformité ne peut être effectuée. C'est le cas si un contrôle utilise AWS Config ou AWS Security Hub comme type de source de données mais que vous n'avez pas activé ces services. C'est également le cas si le contrôle utilise un type de source de données qui ne prend pas en charge les contrôles de conformité, tels que les preuves manuelles, les appels d' AWS API ou AWS CloudTrail.

Si les éléments probants ont le statut de vérification de conformité non applicable dans la console, ils sont classés comme non concluants dans le tableau de bord.

Éléments probants conformes

Les éléments probants sont conformes si un contrôle de conformité n'a révélé aucun problème. C'est le cas si Security Hub indique un résultat satisfaisant ou AWS Config un résultat conforme.

Domaines de contrôle

Le tableau de bord introduit le concept de domaine de contrôle. Vous pouvez considérer un domaine de contrôle comme une catégorie générale de contrôles qui n'est pas spécifique à un framework en particulier. Les groupements de domaines de contrôle sont l'une des fonctionnalités les plus puissantes du tableau de bord. Audit Manager met en évidence les contrôles de vos évaluations qui contiennent des éléments probants non conformes et les regroupe par domaine de contrôle. L'utilisation de cette fonctionnalité vous permet de concentrer vos efforts de remédiation sur des domaines spécifiques lorsque vous vous préparez à un audit.

> **Note**
>
> Un domaine de contrôle est différent d'un ensemble de contrôles. Un ensemble de contrôles est un regroupement de contrôles spécifique à un framework qui est généralement défini par un organisme de réglementation. Par exemple, le framework PCI DSS possède un ensemble de contrôles nommé Exigence 8 : identifier et authentifier l'accès aux composants du système. Cet ensemble de contrôles relève du domaine de contrôle de la gestion des identités et des accès.

Cohérence éventuelle des données

Les données du tableau de bord sont finalement cohérentes. Cela signifie que lorsque vous lisez des données du tableau de bord, il se peut que celles-ci ne reflètent pas instantanément les résultats d'une opération d'écriture ou de mise à jour récemment terminée. Si vous revérifiez dans les heures qui suivent, le tableau de bord devrait refléter les données les plus récentes.

Données provenant d'évaluations supprimées et inactives

Le tableau de bord affiche les données des évaluations actives. Si vous supprimez une évaluation ou passez son statut à inactif le jour même où vous consultez le tableau de bord, les données de cette évaluation sont incluses comme suit.

- Évaluations inactives : si l'Audit Manager a collecté des éléments probants pour votre évaluation avant que vous ne la rendiez inactive, ces éléments probants sont inclus dans le décompte du tableau de bord pour ce jour.
- Évaluations supprimées : si l'Audit Manager a collecté des éléments probants pour votre évaluation avant que vous ne les supprimiez, ces éléments probants ne sont pas inclus dans le décompte du tableau de bord pour ce jour.

Éléments du tableau de bord

Les sections suivantes couvrent les différents composants du tableau de bord.

Rubriques

Filtre d'évaluation

Vous pouvez utiliser le filtre d'évaluation pour vous concentrer sur une évaluation active spécifique.

Par défaut, le tableau de bord affiche des données agrégées pour toutes vos évaluations actives. Si vous souhaitez consulter les données d'une évaluation spécifique, vous devez appliquer un filtre d'évaluation. Il s'agit d'un filtre au niveau de la page qui s'applique à tous les widgets du tableau de bord.

Pour appliquer le filtre d'évaluation, sélectionnez une évaluation dans la liste déroulante en haut du tableau de bord. Cette liste affiche jusqu'à 10 de vos évaluations actives. Les évaluations les plus récentes apparaissent en premier. Si vous avez de nombreuses évaluations actives, vous pouvez commencer à saisir le nom d'une évaluation pour la retrouver rapidement. Une fois que vous avez sélectionné une évaluation, le tableau de bord affiche les données de cette évaluation uniquement.

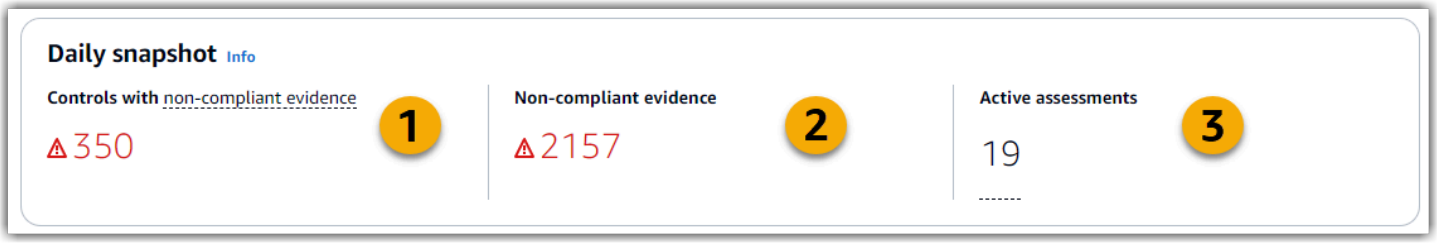
Aperçu quotidien

Ce widget affiche un aperçu de l'état de conformité actuel de vos évaluations actives.

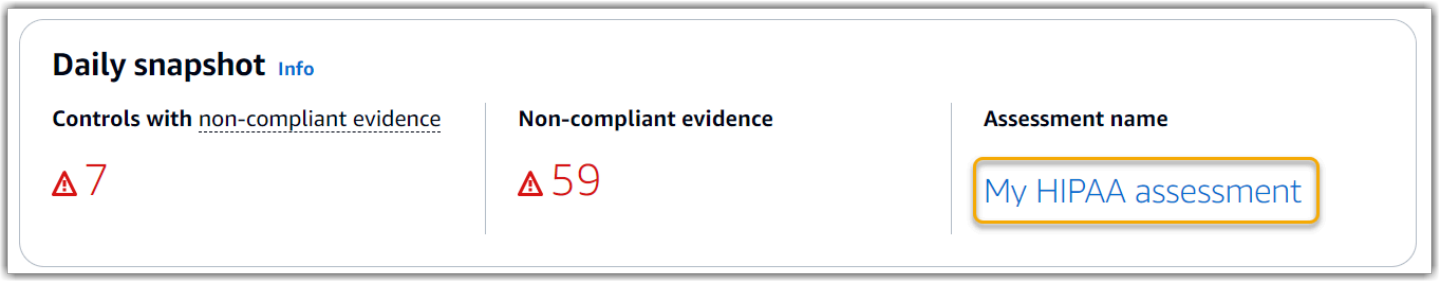
L'aperçu quotidien reflète les dernières données collectées à la date indiquée en haut du tableau de bord. Les dates et heures affichées sur le tableau de bord sont exprimées en heure UTC (temps universel coordonné). Il importe de comprendre que ces chiffres sont des dénombrements quotidiens basés sur cet horodatage. Il ne s'agit pas d'une somme totale à ce jour.

Par défaut, l'aperçu quotidien affiche les données suivantes pour toutes vos évaluations actives :

1. Contrôles comportant des éléments probants non conformes : nombre total de contrôles associés à des éléments probants non conformes.
2. Preuves non conformes - Le nombre total de preuves de contrôle de conformité aboutissant à une conclusion non conforme.
3. Évaluations actives : nombre total de vos évaluations actives. Choisissez ce numéro pour voir les liens vers ces évaluations.



Les données instantanées quotidiennes changent en fonction de the section called "Filtre d'évaluation" ce que vous appliquez. Lorsque vous spécifiez une évaluation, les données reflètent les chiffres quotidiens pour cette évaluation uniquement. Dans ce cas, l'instantané quotidien indique le nom de l'évaluation que vous avez spécifiée. Vous pouvez choisir le nom de l'évaluation pour l'ouvrir.

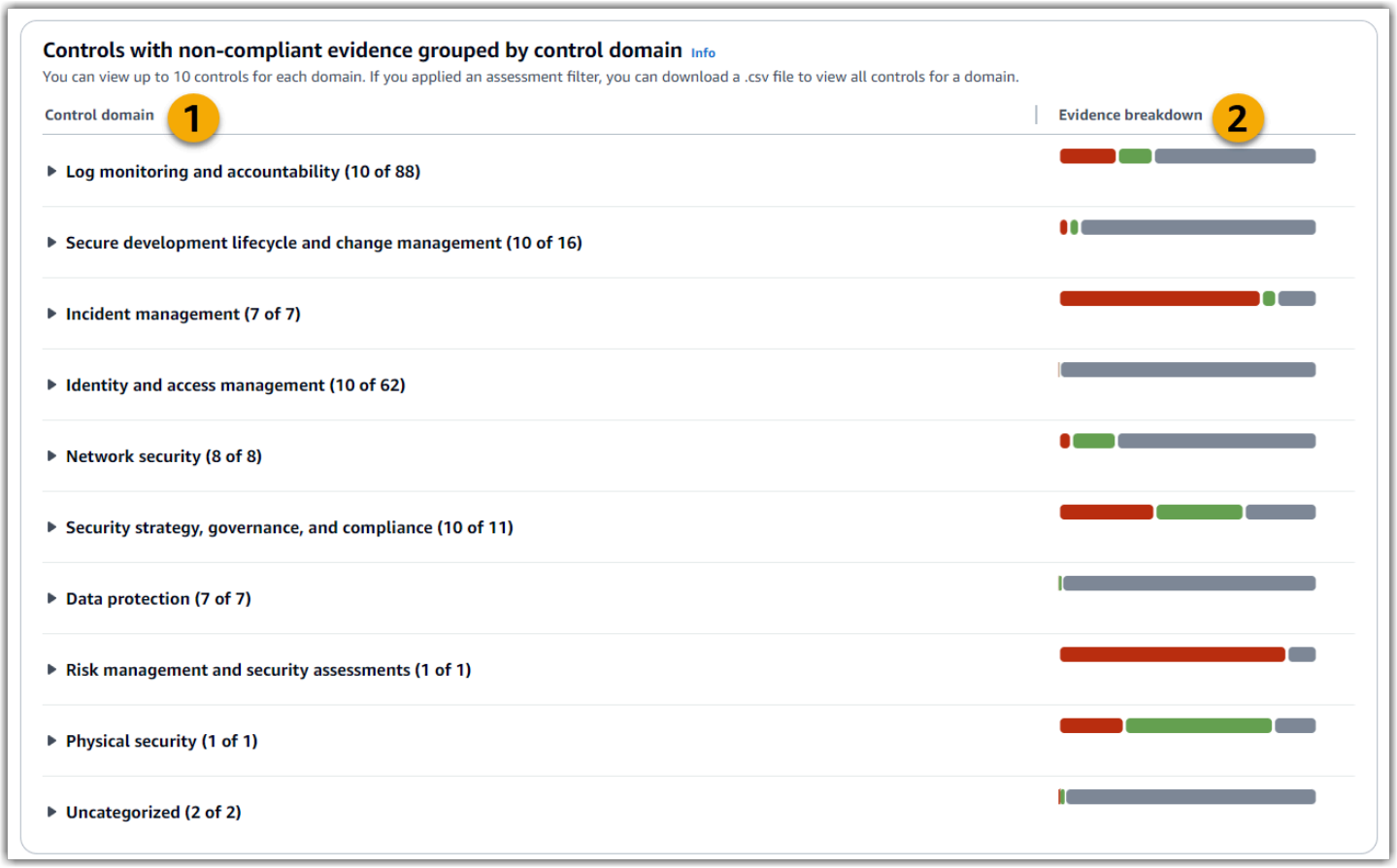


Contrôles comportant des éléments probants non conformes regroupés par domaine de contrôle

Vous pouvez utiliser ce widget pour identifier les contrôles présentant le plus d'éléments probants non conformes.

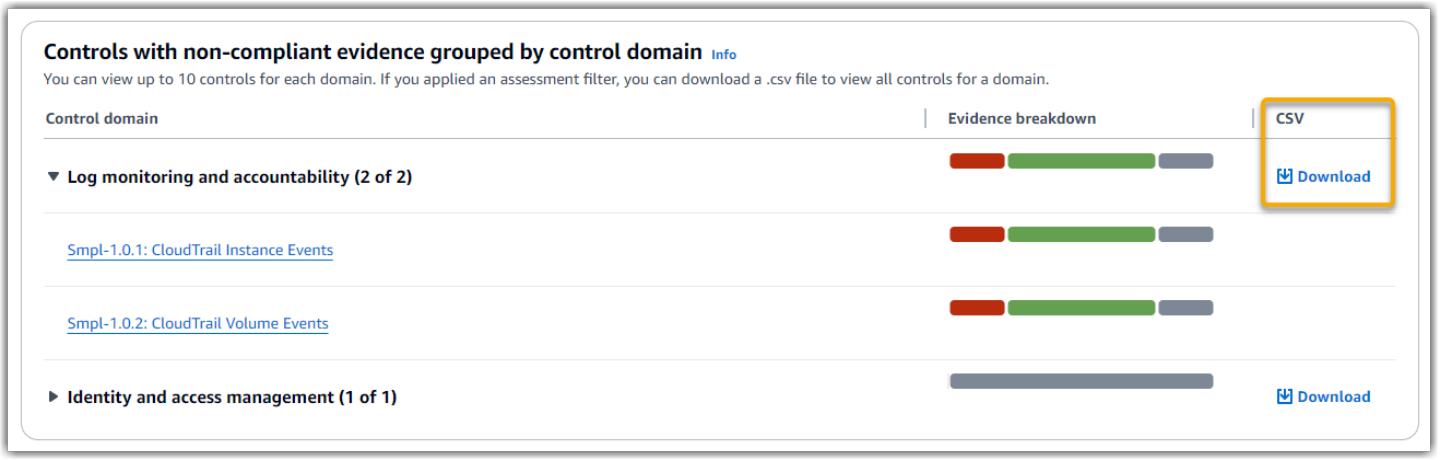
Par défaut, le widget affiche les données suivantes pour toutes vos évaluations actives :

1. Domaine de contrôle : liste control domains des domaines associés à vos évaluations actives.
2. Répartition des éléments probants — Un graphique à barres qui montre une ventilation de l'état de conformité des éléments probants.



Pour développer un domaine de contrôle, choisissez la flèche à côté de son nom. Lorsqu'elle est étendue, la console affiche jusqu'à 10 commandes pour chaque domaine. Ces contrôles sont classés en fonction du nombre total le plus élevé d'éléments probants non conformes.

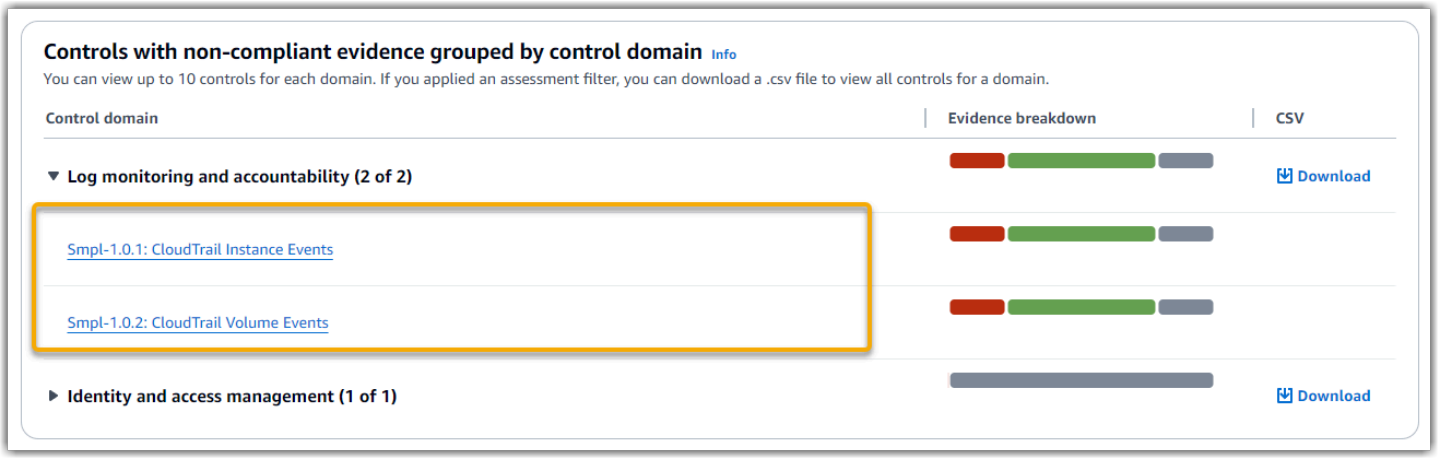
Les données de ce widget changent en fonction de celles the section called "Filtre d'évaluation" que vous appliquez. Lorsque vous spécifiez une évaluation, vous ne voyez que les données de cette évaluation. En outre, vous pouvez également télécharger un fichier CSV pour chaque domaine de contrôle disponible dans l'évaluation.



Le fichier .csv inclut la liste complète des contrôles du domaine qui sont associés à des éléments probants non conformes. L'exemple suivant montre les colonnes de données CSV avec des valeurs fictives.

	A	B	C	D	E	F	G
1	Date and Time	AssessmentID	AsessmentName	ControlId	ControlName	ControlDescription	DataSource
2	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	abcdefgh-1234-bcde-5678-cdefghijklmn	Control 1	Description of control 1	Manual
3	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	12345678-abcd-9012-bcde-345678901234	Control 2	Description of control 2	Manual
4	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	bcdefghi-2345-cdef-3456-defghijklmno	Control 3	Description of control 3	AWS Config, AWS Security Hub
5	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	23456789-bcde-0123-cdef-456789012345	Control 4	Description of control 4	Manual
6	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	cdefghij-3456-defg-4567-efghijklmnop	Control 5	Description of control 5	AWS Config
7	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	34567890-cdef-1234-defg-567890123456	Control 6	Description of control 6	Manual
8	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	defghijk-4567-efgh-5678-fghijklmnopq	Control 7	Description of control 7	AWS Config
9	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	45678901-defg-2345-efgh-678901234567	Control 8	Description of control 8	AWS Security Hub
10	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	efghijkl-5678-fghi-6789-ghijklmnopqr	Control 9	Description of control 9	Manual
11	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	56789012-efgh-3456-fghi-789012345678	Control 10	Description of control 10	Manual
12	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	fghijklm-6789-ghij-7890-hijklmnopqrs	Control 11	Description of control 11	Manual
13	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	67890123-fghi-4567-ghij-890123456789	Control 12	Description of control 12	Manual
14	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	ghijklmn-7890-hijk-8901-ijklmnopqrst	Control 13	Description of control 13	AWS Config, AWS Security Hub
15	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	78901234-ghij-5678-hijk-901234567890	Control 14	Description of control 14	Manual
16							

Enfin, lorsque vous appliquez un filtre d'évaluation, les noms de contrôle sous chaque domaine sont associés à des liens hypertextes. Choisissez n'importe quel contrôle pour ouvrir la page des détails du contrôle dans l'évaluation spécifiée.



> **Tip**
>
> En utilisant la page des détails du contrôle comme point de départ, vous pouvez passer d'un niveau de détail à l'autre.
>
> 1. Page de détails du contrôle - Sur cette page, les Onglet Dossiers d'éléments probants dossiers quotidiens de preuves collectés par Audit Manager pour ce contrôle sont répertoriés. Pour plus de détails, choisissez un dossier.
> 2. Dossier de preuves - Ensuite, vous pouvez consulter une Résumé du dossier d'éléments probants et une liste des preuves contenues dans ce dossier. Pour obtenir plus de détails, sélectionnez un élément probant individuel.
> 3. Élément probant individuel - Enfin, vous pouvez explorer les détails des éléments probants individuels. Il s'agit du niveau d'élément probant le plus granulaire.

Étapes suivantes

Voici les prochaines étapes que vous pouvez suivre après avoir consulté le tableau de bord.

- Téléchargez un fichier CSV : recherchez le domaine d'évaluation et de contrôle sur lequel vous souhaitez vous concentrer, et téléchargez la liste complète des contrôles associés comportant des preuves de non-conformité.
- Révision d'un contrôle : une fois que vous avez identifié un contrôle nécessitant une correction, vous pouvez le réviser.
- Déléguer un contrôle pour révision : si vous avez besoin d'aide pour réviser un contrôle, vous pouvez déléguer un ensemble de contrôles pour révision.
- Modifier votre évaluation : si vous souhaitez modifier le champ d'application d'une évaluation active, vous pouvez modifier l'évaluation.
- Mettre à jour le statut de votre évaluation — Si vous souhaitez arrêter de recueillir des preuves pour une évaluation, vous pouvez faire passer le statut de l'évaluation à inactif.

Ressources supplémentaires

Pour trouver des réponses aux questions et problèmes courants, consultez Résolution des problèmes liés au tableau de bord la section Dépannage de ce guide.

Gestion des évaluations dans AWS Audit Manager

Une évaluation Audit Manager est basée sur un cadre, qui est un regroupement de contrôles. En utilisant un cadre comme point de départ, vous pouvez créer une évaluation qui recueille des éléments probants pour effectuer des contrôles dans ce cadre. Dans votre évaluation, vous pouvez également définir le périmètre de votre audit. Cela inclut la spécification Comptes AWS des éléments pour lesquels vous souhaitez recueillir des preuves.

Points clés

Vous pouvez créer une évaluation à partir de n'importe quel framework. Vous pouvez également utiliser un framework standard fourni par Audit Manager. soit créer une évaluation à partir d'un cadre personnalisé que vous avez créé vous-même. Les frameworks standard contiennent des ensembles de contrôle prédéfinis qui prennent en charge une norme ou une réglementation de conformité spécifique. En revanche, les frameworks personnalisés contiennent des contrôles que vous pouvez personnaliser et regrouper en fonction de vos propres besoins.

Lorsque vous créez une évaluation, cela lance la collecte continue d'éléments probants. Au moment de procéder à un audit, vous ou un délégué pouvez examiner ces preuves, puis les ajouter à un rapport d'évaluation.

> **Note**
>
> AWS Audit Manager aide à recueillir des preuves pertinentes pour vérifier la conformité aux normes et réglementations de conformité spécifiques. Cependant, il n'évalue pas votre conformité lui-même. Les preuves collectées par ce biais peuvent AWS Audit Manager donc ne pas inclure toutes les informations relatives à votre AWS utilisation nécessaires aux audits. AWS Audit Manager ne remplace pas un conseiller juridique ou un expert en conformité.

Ressources supplémentaires

Pour créer et gérer des évaluations dans Audit Manager, suivez les procédures décrites ici.

- Création d'une évaluation dans AWS Audit Manager
- Trouver vos évaluations dans AWS Audit Manager

Création d'une évaluation dans AWS Audit Manager

Cette rubrique s'appuie sur leTutoriel pour les responsables d'audit : création d'une évaluation. Vous trouverez sur cette page des instructions détaillées qui vous montrent comment créer une évaluation à partir d'un framework. Suivez ces étapes pour créer une évaluation et commencer la collecte continue d'éléments probants.

Prérequis

Avant de commencer ce didacticiel, assurez-vous de remplir les conditions suivantes :

- Vous avez rempli tous les prérequis décrits dans Configuration AWS Audit Manager avec les paramètres recommandés. Vous devez utiliser votre console Compte AWS et celle d'Audit Manager pour terminer ce didacticiel.
- Votre identité IAM dispose des autorisations appropriées pour créer et gérer une évaluation dans Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Tâches

- Étape 1 : Indiquer les détails de l'évaluation
- Étape 2 : Spécifier le champ Comptes AWS d'application
- Étape 3 : Spécifier les responsables de l'audit
- Étape 4 : vérifier et créer

Étape 1 : Indiquer les détails de l'évaluation

Commencez par sélectionner un cadre et fournissez des informations de base pour votre évaluation.

Pour indiquer les détails de l'évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations, puis choisissez Créer une évaluation.
3. Sous Nom, saisissez le nom de votre évaluation.
4. (Facultatif) Sous Description, entrez une description pour votre évaluation.
5. Sous Destination des rapports d'évaluation, sélectionnez le compartiment S3 dans lequel vous souhaitez enregistrer vos rapports d'évaluation.

> **Tip**
>
> La destination par défaut du rapport d'évaluation est basée sur vos paramètres d'évaluation. Si vous préférez, vous pouvez créer et utiliser plusieurs compartiments S3 pour vous aider à organiser vos rapports d'évaluation pour les différentes évaluations.

6. Sous Sélectionner le cadre, sélectionnez le cadre à partir duquel vous souhaitez créer votre évaluation. Vous pouvez également utiliser la barre de recherche pour rechercher une structure par son nom, ou par norme ou réglementation de conformité.

> **Tip**
>
> Pour en savoir plus sur un framework, choisissez le nom du framework pour voir la page de détails du framework.

7. (Facultatif) Sous Balises, choisissez Ajouter une nouvelle étiquette pour associer une balise à votre évaluation. Vous pouvez indiquer une clé et une valeur pour chaque balise. La clé de balise est obligatoire et peut être utilisée comme critère de recherche lorsque vous recherchez cette évaluation.
8. Choisissez Suivant.

> **Note**
>
> Il est important de vous assurer que votre évaluation recueille les éléments probants appropriés pour un cadre donné. Avant de commencer la collecte de preuves, nous vous recommandons de passer en revue les exigences du cadre que vous avez choisi. Ensuite, validez ces exigences par rapport aux paramètres de votre AWS Config règle actuelle. Pour vous assurer que vos paramètres de règle sont conformes aux exigences du cadre, vous pouvez mettre à jour la règle dans AWS Config.
> Supposons, par exemple, que vous créez une évaluation pour CIS v1.2.0. Ce framework possède un contrôle nommé 1.9 : assurez-vous que la politique de mot de passe IAM nécessite une longueur minimale de 14 ou plus. Dans AWS Config, la iam-password-policyrègle comporte un `MinimumPasswordLength` paramètre qui vérifie la longueur du mot de passe. La valeur par défaut de ce paramètre est de 14 caractères. Par conséquent, la règle s'aligne sur les exigences de contrôle. Si vous n'utilisez pas la valeur de paramètre par défaut, assurez-vous que la valeur que vous utilisez est égale ou supérieure aux

14 caractères requis par CIS v1.2.0. Vous trouverez les détails des paramètres par défaut pour chaque règle gérée dans la documentation AWS Config.

Étape 2 : Spécifier le champ Comptes AWS d'application

Vous pouvez en spécifier plusieurs Comptes AWS pour qu'ils soient inclus dans le champ d'une évaluation. Audit Manager prend en charge plusieurs comptes grâce à l'intégration à AWS Organizations. Cela signifie que les évaluations d'Audit Manager peuvent être effectuées sur plusieurs comptes et que les preuves collectées sont consolidées dans un compte d'administrateur délégué. Pour activer Organisations dans Audit Manager, veuillez consulter Activer et configurer AWS Organizations (facultatif).

> **Note**
>
> Audit Manager peut prendre en charge jusqu'à 200 comptes dans le cadre d'une évaluation. Si vous essayez d'inclure plus de 200 comptes, la création de l'évaluation risque d'échouer.

Pour spécifier Comptes AWS dans le champ d'application

1. Sous Comptes AWS, sélectionnez les éléments Comptes AWS que vous souhaitez inclure dans le champ de votre évaluation.
   - Si vous avez activé Organisations dans Audit Manager, plusieurs comptes sont affichés. Vous pouvez sélectionner un ou plusieurs comptes dans la liste. Vous pouvez également rechercher un compte à l'aide de son nom, de son identifiant ou de son adresse e-mail.
   - Si vous n'avez pas activé Organizations dans Audit Manager, seule votre version actuelle Compte AWS est répertoriée.
2. Choisissez Suivant.

> **Note**
>
> Lorsqu'un compte concerné est supprimé de votre organisation, Audit Manager ne collecte plus d'éléments probants pour ce compte. Cependant, le compte continue d'apparaître dans votre évaluation sous l'onglet Comptes AWS. Pour supprimer le compte de la liste des comptes concernés, modifiez l'évaluation. Le compte supprimé n'apparaît plus dans la liste

lors de la modification et vous pouvez enregistrer vos modifications sans que ce compte soit concerné.

Étape 3 : Spécifier les responsables de l'audit

Dans cette étape, vous indiquez les responsables de l'audit pour votre évaluation. Les responsables de l'audit sont les personnes de votre lieu de travail, généralement issues de la GRC ou d' DevOps équipes SecOps, qui sont chargées de gérer l'évaluation de l'Audit Manager. Nous leur recommandons d'utiliser cette AWSAuditManagerAdministratorAccesspolitique.

Pour indiquer les responsables de l'audit

1. Sous Responsables de l'audit, consultez la liste actuelle des responsables de l'audit. La colonne Responsable de l'audit affiche les ID utilisateur et les rôles. La Compte AWScolonne indique le nom Compte AWS du propriétaire de l'audit.
2. Les responsables de l'audit pour lesquels une case est cochée sont inclus dans votre évaluation. Décochez la case correspondant à tout responsable de l'audit afin de le supprimer de l'évaluation. Vous pouvez trouver d'autres responsables d'audit en utilisant la barre de recherche pour effectuer une recherche par nom ou Compte AWS.
3. Lorsque vous avez terminé, choisissez Suivant.

Étape 4 : vérifier et créer

Vérifiez les informations de votre évaluation. Pour modifier les informations d'une étape, choisissez Modifier. Lorsque vous avez terminé, choisissez Créer une évaluation.

Cette action lance la collecte continue d'éléments probants pour votre évaluation. Une fois que vous avez créé une évaluation, la collecte d'éléments probants se poursuit jusqu'à ce que vous passiez le statut de l'évaluation à inactif. Vous pouvez également arrêter la collecte de preuves pour un contrôle spécifique en faisant passer le statut du contrôle à inactif.

> **Note**
>
> Les preuves automatisées sont disponibles 24 heures après la création de votre évaluation. Audit Manager collecte automatiquement des éléments probants à partir de plusieurs sources de données, et la fréquence de cette collecte d'éléments probants est basée sur le type

d'éléments probants. Pour de plus amples informations, veuillez consulter Fréquence de collecte des éléments probants dans le présent guide.

Étapes suivantes

Pour revoir votre évaluation à une date ultérieure, consultezTrouver vos évaluations dans AWS Audit Manager. Vous pouvez suivre ces étapes pour localiser votre évaluation afin de pouvoir la consulter, la modifier ou continuer à travailler dessus.

Ressources supplémentaires

Pour des solutions aux problèmes d'évaluation dans Audit Manager, consultezRésolution des problèmes liés aux évaluations et à la collecte d'éléments probants.

Trouver vos évaluations dans AWS Audit Manager

Après avoir créé des évaluations dans AWS Audit Manager, vous pouvez les trouver sur la page des évaluations de la console Audit Manager.

À partir de cette page, vous pouvez effectuer différentes actions sur vos évaluations. Par exemple, vous pouvez consulter les détails de l'évaluation, modifier les configurations d'évaluation ou supprimer les évaluations qui ne sont plus nécessaires. En outre, la page des évaluations sert de point de départ pour créer de nouvelles évaluations.

Vous pouvez également consulter vos évaluations par programmation à l'aide de l'API Audit Manager ou du AWS Command Line Interface ()AWS CLI.

Prérequis

La procédure suivante suppose que vous avez déjà créé au moins une évaluation. Si vous n'avez pas encore créé d'évaluation, vous ne verrez aucun résultat si vous suivez ces étapes.

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour consulter une évaluation dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Vous pouvez consulter vos évaluations à l'aide de la console Audit Manager, de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

Audit Manager console

Pour consulter vos évaluations sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Évaluations pour afficher la liste de vos évaluations.
3. Choisissez un nom d'évaluation pour afficher les détails de cette évaluation.

AWS CLI

Pour afficher vos évaluations (CLI)

Pour consulter les évaluations dans Audit Manager, exécutez la commande list-assessments. Vous pouvez utiliser la sous-commande `--status` pour afficher les évaluations actives ou inactives.

```
aws auditmanager list-assessments --status ACTIVE
```

```
aws auditmanager list-assessments --status INACTIVE
```

Audit Manager API

Pour consulter vos évaluations à l'aide de l'API

Pour consulter les évaluations dans Audit Manager, utilisez l'ListAssessmentsopération. Vous pouvez utiliser l'attribut statut pour afficher les évaluations actives ou inactives.

Pour plus d'informations, choisissez l'un des liens précédents pour en lire davantage dans le Guide de référence de l'API AWS Audit Manager . Il inclut des informations sur l'utilisation du fonctionnement et des paramètres `ListAssessments` dans l'un des SDK AWS spécifiques au langage.

Étapes suivantes

Lorsque vous êtes prêt à explorer le contenu de votre évaluation, suivez les étapes décrites dansRévision d'une évaluation dans AWS Audit Manager. Cette page vous guidera à travers les détails de l'évaluation et expliquera les informations que vous y trouverez.

Sur la page des évaluations, vous pouvez également modifier une évaluation, supprimer une évaluation ou créer une évaluation.

Ressources supplémentaires

Pour des solutions aux problèmes d'évaluation dans Audit Manager, consultezRésolution des problèmes liés aux évaluations et à la collecte d'éléments probants.

Révision d'une évaluation dans AWS Audit Manager

Après avoir créé des évaluations dans Audit Manager, vous pouvez les ouvrir et les consulter à tout moment.

Points clés

Lorsque vous êtes prêt à explorer votre évaluation, vous pouvez progressivement approfondir les détails et revoir votre évaluation avec des niveaux de granularité croissants.

1. Détails de l'évaluation — Commencez par examiner les détails généraux de votre évaluation. Sur cette page, vous pouvez consulter le nom, la description, le champ d'application et d'autres détails de l'évaluation. Cela vous donne une vue d'ensemble de haut niveau de l'évaluation.
2. Détails du contrôle d'évaluation — Ensuite, approfondissez l'évaluation en examinant les détails de chaque contrôle d'évaluation. Cela vous permettra de comprendre les exigences et les objectifs spécifiques de chaque contrôle.
3. Détails du dossier de preuves — Pour chaque contrôle d'évaluation, vous pouvez consulter les dossiers de preuves correspondants qui contiennent les preuves d'un contrôle donné. Ces dossiers organisent les preuves justificatives liées à chaque contrôle.
4. Détails des preuves — Enfin, approfondissez votre recherche pour passer en revue les différents éléments de preuve contenus dans chaque dossier. Cela peut inclure des instantanés de configuration, des journaux d'activité des utilisateurs, des résultats de conformité ou des preuves téléchargées manuellement, telles que des documents et des captures d'écran. L'examen de ces

preuves vous aidera à comprendre dans quelle mesure votre organisation répond aux exigences du contrôle.

En suivant ces étapes, vous pouvez explorer en profondeur votre évaluation, comprendre ses composantes et examiner les preuves qui soutiennent les efforts de conformité de votre organisation.

Ressources supplémentaires

Pour commencer à examiner une évaluation dans Audit Manager, suivez les procédures décrites ici.

- Consulter les détails de l'évaluation dans AWS Audit Manager
- Révision d'un contrôle d'évaluation dans AWS Audit Manager
- Révision d'un dossier de preuves dans AWS Audit Manager
- Examen des preuves dans AWS Audit Manager

Consulter les détails de l'évaluation dans AWS Audit Manager

Lorsque vous devez examiner les détails d'une évaluation, vous trouverez les informations organisées en plusieurs sections sur la page des détails de l'évaluation. Ces sections vous aident à accéder facilement aux informations pertinentes pour votre tâche et à les comprendre.

Table des matières

Prérequis

La procédure suivante suppose que vous avez déjà créé au moins une évaluation. Si vous n'avez pas encore créé d'évaluation, vous ne verrez aucun résultat si vous suivez ces étapes.

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour consulter une évaluation dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Pour ouvrir et consulter la page de détails d'une évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Évaluations pour afficher la liste de vos évaluations.
3. Choisissez le nom de l'évaluation pour l'ouvrir.
4. Passez en revue les détails de l'évaluation en utilisant les informations suivantes comme référence.

Sections de la page de détails de l'évaluation

- Section des détails de l'évaluation
- Onglet Contrôles
- Onglet de sélection du rapport d'évaluation
- Comptes AWS onglet
- Services AWS onglet
- Onglet des responsables de l'Audit
- Onglet Balises
- Onglet Journal des modifications

Section des détails de l'évaluation

Vous pouvez utiliser la section Détails de l'évaluation pour voir un résumé de votre évaluation.

Dans la section des détails de l'évaluation, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
1. Description	Description de l'évaluation.
2. Type de conformité	Norme ou réglementation de conformité prise en charge par l'évaluation.
3. Destination des rapports d'évaluation	Le compartiment S3 dans lequel Audit Manager enregistre le rapport d'évaluation.
4. Preuve totale	Le nombre total d'éléments de preuve collectés pour cette évaluation.
5. Sélection du rapport d'évaluation	Le nombre d'éléments de preuve sélectionnés pour être inclus dans le rapport d'évaluation.
6. Date de création	Date à laquelle l'évaluation a été créée.
7. Dernière mise à jour	Date à laquelle l'évaluation a été modifiée pour la dernière fois.
8. Statut	État de l'évaluation. • Actif - L'évaluation recueille actuellement des preuves. • Inactif - L'évaluation ne recueille plus de preuves.

Onglet Contrôles

Vous pouvez utiliser cet onglet pour consulter les informations relatives aux contrôles de l'évaluation.

Sous Résumé de l'état du contrôle, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
Contrôles complets	Le nombre total de contrôles inclus dans cette évaluation.
Révisé	Le nombre de contrôles qui ont été examinés par un responsable de l'audit ou un délégué.
En cours de révision	Le nombre de contrôles actuellement en cours de révision.
Inactif	Le nombre de contrôles qui ne collectent plus activement des preuves

Dans le tableau des ensembles de contrôles, vous pouvez consulter la liste des contrôles regroupés par ensemble de contrôles. Vous pouvez étendre ou réduire les contrôles de chaque ensemble de contrôles. Vous pouvez également effectuer une recherche par nom si vous recherchez un contrôle spécifique.

Dans ce tableau, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
Contrôles regroupés par ensembles de commandes	Nom du jeu de commandes.
État du contrôle	État du contrôle. • En cours de vérification indique que ce contrôle n'a pas encore été vérifié. Des preuves sont toujours en cours de collecte pour ce contrôle, et vous pouvez ajouter des preuves manuelles. Il s'agit du statut par défaut. • Vérifié indique que les éléments probants de ce contrôle ont été vérifiés. Les preuves sont toujours en cours de collecte et vous pouvez ajouter des preuves manuelles.

Name (Nom)	Description
	• Inactif indique que la collecte automatique de preuves est arrêtée pour ce contrôle. Vous ne pouvez plus ajouter de preuves manuelles.
Délégué à	Le réviseur de ce contrôle, s'il a été attribué à un délégué pour révision.
Preuve totale	Le nombre d'éléments de preuve qui ont été collectés pour ce contrôle.

Onglet de sélection du rapport d'évaluation

Vous pouvez utiliser cet onglet pour voir les preuves qui seront incluses dans le rapport d'évaluation. Les preuves sont regroupées par dossiers de preuves, organisés en fonction de la date à laquelle elles ont été créées.

Vous pouvez parcourir ces dossiers et sélectionner les éléments probants que vous souhaitez inclure dans votre rapport d'évaluation. Pour obtenir des instructions sur la façon d'ajouter des preuves à un rapport d'évaluation, voirAjouter des éléments probants à un rapport d'évaluation.

Dans cette section, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
Dossier de preuves	Le nom du dossier de preuves. Le nom du dossier est basé sur la date à laquelle les éléments probants ont été collectés.
Éléments de preuve sélectionnés	Le nombre d'éléments de preuve contenus dans le dossier qui sont inclus dans le rapport d'évaluation.
Nom du contrôle	Nom du contrôle associé à ce dossier de preuves.

Comptes AWS onglet

Vous pouvez utiliser cet onglet pour voir ceux Comptes AWS qui entrent dans le champ d'application de l'évaluation.

Dans cette section, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
ID de compte	ID du Compte AWS.
Nom du compte	Le nom de l' Compte AWS.
E-mail	Indiquez l'adresse e-mail associée au Compte AWS.

Services AWS onglet

Il est possible que cet onglet apparaisse ou non dans votre évaluation.

Si l' Services AWS onglet n'est pas affiché (état idéal)

Si vous ne voyez pas cet onglet, cela signifie qu'Audit Manager gère Services AWS les éléments concernés par votre évaluation.

Audit Manager déduit cette portée en examinant vos contrôles d'évaluation et leurs sources de données, puis en mappant ces informations aux informations correspondantes Services AWS. Chaque fois qu'une source de données sous-jacente change pour votre évaluation, Audit Manager met automatiquement à jour l'étendue selon les besoins pour refléter la bonne Services AWS. Cela garantit que votre évaluation recueille des preuves précises et complètes sur tous les services pertinents de votre AWS environnement.

Si l' Services AWS onglet est affiché

Si tel est le cas, cet onglet indique qu'Audit Manager ne gère pas Services AWS les éléments concernés par votre évaluation.

Dans ce cas, les informations suivantes concernant les services concernés par le champ d'application que vous avez défini s'affichent :

Name (Nom)	Description
Service AWS	Le nom de l' Service AWS.
Catégorie	Catégorie de service, telle que le calcul ou la base de données.

Name (Nom)	Description
Description	Description de la Service AWS.

Audit Manager effectue des évaluations des ressources pour les services figurant dans ce tableau. Par exemple, si Amazon S3 est répertorié, Audit Manager peut collecter des éléments probants concernant vos compartiments S3. Les preuves exactes collectées sont déterminées par celles d'un contrôledata source. Par exemple, si le type de source de données est AWS Config et que le mappage des sources de données est une AWS Config règle (telle que`s3-bucket-public-write-prohibited`), Audit Manager collecte le résultat de cette évaluation des règles à titre de preuve. Pour plus d'informations, consultez Quelle est la différence entre un service concerné et un type de source de données ? dans ce guide.

Si votre évaluation a été créée dans la console à partir d'un cadre standard, Audit Manager a sélectionné les services pour vous et a mappé leurs sources de données conformément aux exigences du cadre. Si le cadre standard ne contient que des commandes manuelles, aucune n'entre Services AWS dans le champ d'application.

> **Note**
>
> La prochaine fois que vous modifierez votre évaluation ou modifierez l'un des contrôles personnalisés de votre évaluation, Audit Manager prendra en charge la gestion des services concernés pour vous. Dans ce cas, l'Services AWSonglet est supprimé de votre évaluation.

Onglet des responsables de l'Audit

Vous pouvez utiliser cet onglet pour voir les responsables de l'audit pour l'évaluation.

Dans cette section, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
Responsable de l'audit	Nom du responsable de l'audit.
Compte AWS	Compte AWS ID du propriétaire de l'audit.

Onglet Balises

Vous pouvez utiliser cet onglet pour voir les balises associées à votre évaluation. Ces balises sont héritées du framework utilisé pour créer l'évaluation. Pour plus d'informations sur les balises dans l'Audit Manager, veuillez consulter Ressources de balisage AWS Audit Manager.

Dans cette section, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
Clé	La clé de la balise, telle qu'une norme de conformité, une réglementation ou une catégorie.
Valeur	Valeur de la balise.

Onglet Journal des modifications

Vous pouvez utiliser cet onglet pour voir l'activité des utilisateurs dans le cadre de l'évaluation.

Dans cette section, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
Date	Date de l'activité.
Utilisateur	L'utilisateur qui a effectué l'action.
Action	L'action qui s'est produite, telle qu'une évaluation en cours de création.
Type	Type d'objet qui a changé, par exemple une évaluation.
Ressource	La ressource affectée par le changement, telle que le cadre à partir duquel l'évaluation a été créée.

Étapes suivantes

Pour continuer à consulter le contenu de votre évaluation, suivez les étapes décrites dansRévision d'un contrôle d'évaluation dans AWS Audit Manager. Cette page vous guidera à travers les détails du contrôle d'évaluation et expliquera les informations que vous y trouverez.

Ressources supplémentaires

- Sur la page des détails de mon évaluation, je suis invité à recréer mon évaluation
- Je ne vois aucun contrôle ou ensemble de contrôles dans mon évaluation
- Je ne vois pas les services concernés par mon évaluation

Révision d'un contrôle d'évaluation dans AWS Audit Manager

Lorsque vous devez passer en revue les contrôles d'une évaluation, vous trouverez les informations organisées en plusieurs sections sur la page des détails des contrôles d'évaluation. Ces sections vous aident à accéder facilement aux informations pertinentes pour votre tâche et à les comprendre.

Table des matières

Prérequis

La procédure suivante suppose que vous avez déjà créé au moins une évaluation. Si vous n'avez pas encore créé d'évaluation, vous ne verrez aucun résultat si vous suivez ces étapes.

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour consulter une évaluation dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Pour ouvrir et consulter la page de détails d'un contrôle d'évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Assessments et choisissez le nom d'une évaluation pour l'ouvrir.
3. Sur la page d'évaluation, choisissez l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'au tableau des Ensembles de contrôles, puis choisissez le nom d'un contrôle pour l'ouvrir.
4. Passez en revue les détails du contrôle de l'évaluation en utilisant les informations suivantes comme référence.

Sections de la page détaillée des contrôles d'évaluation

- Section des détails du contrôle
- Onglet Dossiers d'éléments probants
- Onglet Détails
- Onglet Sources de preuves
- Onglet des commentaires
- Onglet Journal des modifications

Section des détails du contrôle

Vous pouvez utiliser la section Détails du contrôle pour voir un résumé du contrôle d'évaluation.

Dans cette section, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
Description	Description fournie pour ce contrôle.

Name (Nom)	Description
État du contrôle	État du contrôle. • En cours de révision — Le contrôle n'a pas encore été révisé. Des preuves sont toujours en cours de collecte pour ce contrôle, et vous pouvez ajouter des preuves manuelles. Il s'agit du statut par défaut. • Révisé — Les preuves de ce contrôle sont passées en revue. Les preuves sont toujours en cours de collecte et vous pouvez ajouter des preuves manuelles. • Inactif — La collecte automatique de preuves est interromp ue pour ce contrôle. Vous ne pouvez plus ajouter de preuves manuelles.

Onglet Dossiers d'éléments probants

Vous pouvez utiliser cet onglet pour voir les preuves collectées pour ce contrôle. Il est organisé en dossiers sur une base quotidienne. À partir de là, vous pouvez également effectuer les actions suivantes :

- Consulter un dossier de preuves : pour voir les détails d'un dossier de preuves, choisissez le nom du dossier en lien hypertexte.
- Ajouter un dossier de preuves à un rapport d'évaluation : pour inclure un dossier de preuves, sélectionnez-le et choisissez Ajouter au rapport d'évaluation.
- Supprimer un dossier de preuves d'un rapport d'évaluation : pour exclure un dossier, sélectionnez-le et choisissez Supprimer du rapport d'évaluation.
- Ajouter des preuves manuelles — Pour les instructions, voirAjouter des preuves manuelles dans AWS Audit Manager.

Dans cette section, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
Dossier de preuves	Le nom du dossier de preuves. Le nom est basé sur la date à laquelle les éléments probants ont été collectés ou ajoutés manuellement.
Contrôle de conformité	Le nombre de points figurant dans le dossier de preuves. Ce nombre représente le nombre total de problèmes de sécurité qui ont été signalés directement par AWS Security Hub AWS Config, ou par les deux. Si la mention Non applicable s'affiche, cela signifie que Security Hub n'est pas AWS Config activé ou que les preuves proviennent d'un autre type de source de données.
Preuve totale	Le nombre total d'éléments de preuve contenus dans le dossier.
Sélection du rapport d'évaluation	Le nombre d'éléments de preuve contenus dans le dossier qui sont inclus dans le rapport d'évaluation.

> **Tip**
>
> Si vous ne trouvez pas le dossier de preuves que vous recherchez, remplacez le filtre déroulant par Tout le temps. Dans le cas contraire, les dossiers des sept derniers jours s'afficheront par défaut.

Onglet Détails

Dans cette section, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
Informations sur les tests	Procédure recommandée pour vérifier que le contrôle fonctionne comme prévu.

Name (Nom)	Description
Plan d'action	Les mesures recommandées à prendre si le contrôle doit être corrigé.

Onglet Sources de preuves

Vous pouvez utiliser cet onglet pour voir d'où le contrôle d'évaluation collecte les preuves. Les sources de preuves peuvent inclure n'importe laquelle des sources suivantes :

Name (Nom)	Description
Contrôles communs	Il s'agit des contrôles courants qui collectent des preuves à l'appui du contrôle d'évaluation. Les contrôles courants collectent des preuves à l'aide de sources de données sous-jacentes AWS gérées pour vous. Pour chaque contrôle commun répertorié, Audit Manager collecte les preuves pertinentes pour tous les contrôles de base sous-jacents. Choisisse z un contrôle commun pour voir les contrôles principaux associés.
Contrôles de base	Il s'agit des contrôles de base qui collectent des preuves à l'appui du contrôle d'évaluation. Les contrôles de base collectent des preuves à l'aide d'un groupe prédéfini de sources de données qui se AWS gèrent pour vous. Choisissez un contrôle principal pour voir les sources de données sous-jacentes.
Sources de données	Il s'agit des sources de données individuelles qui collectent des preuves à l'appui du contrôle de l'évaluation. • Nom : nom de la source de données. • Type : type de source de données d'où proviennent les preuves. • Si Audit Manager collecte les preuves, le type peut être AWS Security Hub, AWS ConfigAWS CloudTrail, ou des appels AWS d'API.

Name (Nom)	Description

	• Si vous téléchargez vos propres preuves, le type est Manuel. Une description indique si l'élément probant manuel requis est un Chargement de fichier ou une Réponse sous forme de texte.
	• Cartographie : mot clé spécifique utilisé pour collecter des preuves.
	  • Si c'est le cas AWS Config, le mappage est une AWS Config règle (telle que`SNS_ENCRYPTED_KMS`)
	  • Si c'est le cas AWS Security Hub, le mappage est un contrôle Security Hub (tel que`EC2.1`).
	  • Si le type est un appel AWS d'API, le mappage est un appel d'API (tel que`kms_ListKeys`).
	  • Si c'est le cas AWS CloudTrail, le mappage est un CloudTrail événement (tel que`CreateAccessKey`).
	• Fréquence : fréquence à laquelle Audit Manager collecte des preuves relatives à une source de données d'appel d' AWS API.

Onglet des commentaires

Dans cet onglet, vous pouvez ajouter un commentaire sur le contrôle et ses preuves. Vous pouvez également consulter la liste des commentaires précédents.

- Sous Envoyer des commentaires, vous pouvez ajouter des commentaires pour un contrôle en saisissant du texte, puis en choisissant Soumettre les commentaires.
- Sous Commentaires précédents, vous pouvez consulter la liste des commentaires précédents ainsi que la date à laquelle chaque commentaire a été publié et le nom d'utilisateur associé.

Onglet Journal des modifications

Vous pouvez utiliser cet onglet pour voir l'activité des utilisateurs dans le cadre du contrôle d'évaluation. Les mêmes informations sont disponibles lorsque la piste d'audit se connecte dans AWS CloudTrail. Grâce à l'activité des utilisateurs capturée directement dans Audit Manager, vous pouvez facilement consulter une piste d'audit de l'activité d'un contrôle donné.

Dans cette section, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
Date	Date et heure de l'activité, représentées en temps universel coordonné (UTC).
Utilisateur	L'utilisateur ou le rôle qui a effectué l'activité.
Action	L'action qui s'est produite, telle qu'une évaluation en cours de création.
Type	Type d'objet qui a changé, par exemple une évaluation.
Ressource	La ressource affectée par le changement, telle que le cadre à partir duquel l'évaluation a été créée.

Audit Manager suit les activités des utilisateurs suivantes dans les journaux des modifications :

- Création d'une évaluation
- Modification d'une évaluation
- Complétion d'une évaluation
- Suppression d'une évaluation
- Délégation d'un ensemble de contrôles à des fins d'examen
- Soumission d'un ensemble de contrôles vérifié au responsable de l'audit
- Chargement d'éléments probants manuels
- Mise à jour du statut d'un contrôle
- Génération de rapports d'évaluation

Étapes suivantes

Pour continuer à examiner votre évaluation, suivez les étapes décrites dansRévision d'un dossier de preuves dans AWS Audit Manager. Cette page vous guidera à travers les dossiers de preuves et vous montrera comment comprendre les informations que vous voyez.

Ressources supplémentaires

- Je ne vois aucun contrôle ou ensemble de contrôles dans mon évaluation

Révision d'un dossier de preuves dans AWS Audit Manager

Au fur et à mesure que votre évaluation collecte des preuves, Audit Manager les organise dans des dossiers pour vous faciliter la tâche. Lorsque vous devez consulter un dossier de preuves, vous trouverez les informations organisées en plusieurs sections.

Table des matières

Prérequis

La procédure suivante suppose que vous avez déjà créé au moins une évaluation. Si vous n'avez pas encore créé d'évaluation, vous ne verrez aucun résultat si vous suivez ces étapes.

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour consulter une évaluation dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

N'oubliez pas qu'il faut jusqu'à 24 heures pour qu'une évaluation commence à recueillir des preuves automatisées. Si votre évaluation ne contient pas encore de preuves, vous ne verrez aucun résultat si vous suivez ces étapes.

Procédure

Pour ouvrir et consulter un dossier de preuves

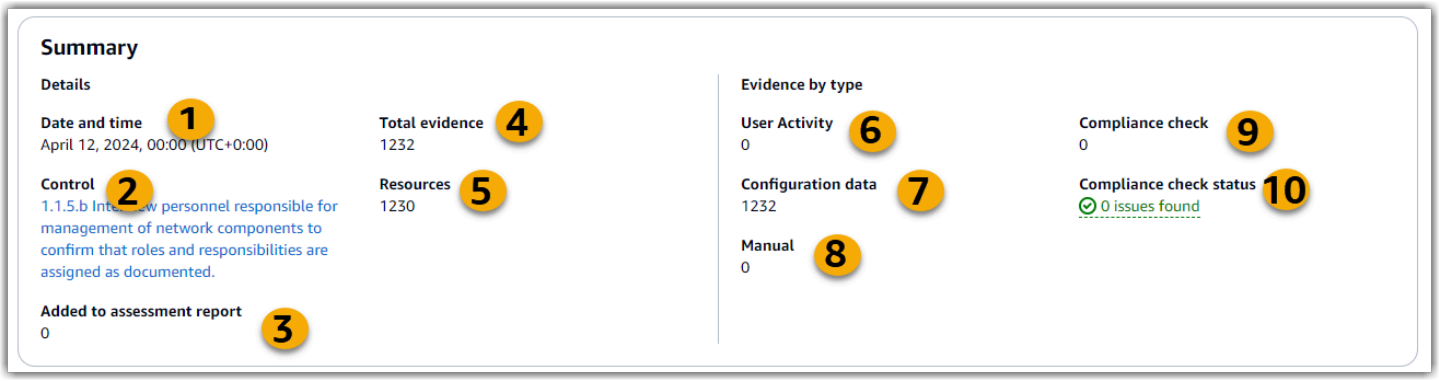
1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, sélectionnez Évaluations, puis choisissez une évaluation.
3. Sur la page d'évaluation, choisissez l'onglet Contrôles, faites défiler la page vers le bas jusqu'au tableau Contrôles, puis choisissez un contrôle d'évaluation.
4. Sur la page de contrôle de l'évaluation, choisissez l'onglet Dossiers de preuves.
5. Dans le tableau Dossiers de preuves, choisissez le nom d'un dossier de preuves.
6. Passez en revue le dossier de preuves en utilisant les informations suivantes comme référence.

Sections d'une page de dossier de preuves

- Résumé du dossier d'éléments probants
- Tableau des éléments probants

Résumé du dossier d'éléments probants

Vous pouvez utiliser la section Résumé de la page pour obtenir un aperçu général des preuves contenues dans le dossier des preuves. Pour en savoir plus sur les différents types de preuves, voir Preuves.



Dans cette section, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
1. Date et heure	Heure et date de création du dossier de preuves. Cela est représenté en temps universel coordonné (UTC).
2. Contrôle	Le nom du contrôle associé au dossier de preuves.
3. Ajouté au rapport d'évaluation	Le nombre d'éléments de preuve sélectionnés pour être inclus dans le rapport d'évaluation.
4. Preuve totale	Le nombre total d'éléments de preuve contenus dans le dossier de preuves.
5. Ressources	Le nombre total de AWS ressources qui ont été évaluées lors de la collecte des preuves contenues dans ce dossier.
6. Activité de l'utilisateur	Le nombre d'éléments de preuve relevant de la catégorie d'activit é de l'utilisateur. Ces preuves sont collectées à partir de AWS CloudTrail journaux.
7. Données de configura tion	Le nombre d'éléments de preuve relevant de la catégorie des données de configuration. Ces preuves sont collectées à partir d'appels d'API qui prennent des instantanés de configuration d'autres Services AWS applications.
8. Manuel	Le nombre d'éléments de preuve relevant de la catégorie des manuels. Ces preuves sont ajoutées manuellement.
9. Contrôle de conformité	Le nombre d'éléments de preuve entrant dans la catégorie des contrôles de conformité. Ces preuves sont recueillies auprès de AWS Config AWS Security Hub, ou des deux.
10. État du contrôle de conformité	Le nombre total de problèmes signalés directement par AWS Security Hub AWS Config, ou par les deux.

Tableau des éléments probants

Vous pouvez utiliser le tableau Preuves pour voir les preuves contenues dans le dossier de preuves. À partir de ce tableau, vous pouvez également effectuer les actions suivantes :

- Examiner les preuves individuelles — Pour voir les détails d'un élément de preuve, choisissez le nom de la preuve hypertexte dans la colonne Heure.
- Ajouter des preuves à un rapport d'évaluation : pour inclure des preuves, sélectionnez-les et choisissez Ajouter au rapport d'évaluation.
- Supprimer des preuves d'un rapport d'évaluation : pour exclure des preuves, sélectionnez-les et choisissez Supprimer du rapport d'évaluation.
- Ajouter des preuves manuelles — Pour les instructions, voirAjouter des preuves manuelles dans AWS Audit Manager.

Dans ce tableau, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
Time (Période)	Spécifie le moment où les preuves ont été collectées. Cela sert également de nom à la preuve. L'heure est représentée au format UTC (temps universel coordonné).
Contrôle de conformité	État d'évaluation des preuves relevant de la catégorie des contrôles de conformité. • Pour les preuves collectées auprès de Security Hub, un résultat de réussite ou d'échec est signalé directement par Security Hub. • Pour les preuves collectées auprès de AWS Config, un résultat conforme ou non conforme est signalé directement à partir de AWS Config. • Si l'option Non applicable apparaît, cela indique que Security Hub n'est pas activé AWS Config ou que les preuves proviennent d'un autre type de source de données.
Preuve par type	Le type de preuve. • Les preuves du contrôle de conformité sont collectées auprès de AWS Config ou AWS Security Hub. • Les preuves de l'activité des utilisateurs sont collectées auprès de AWS CloudTrail.

Name (Nom)	Description
	• Les preuves des données de configuration sont collectées à partir d'appels d'API à d'autres Services AWS. • Les preuves manuelles sont des preuves que vous ajoutez manuellement.
Source de données	Source de données à partir de laquelle les preuves sont collectées.
Nom de l'événement	Le nom de l'événement qui a fait appel à la collecte de preuves.
Source de l'événement	Le principal de service qui identifie les éléments pertinents Service AWS pour l'événement.
Ressources	Le nombre de ressources qui ont été évaluées lors de la collecte des preuves.
Sélection du rapport d'évaluation	Indique si les preuves sont incluses dans le rapport d'évaluation. • Pour inclure des éléments probants, sélectionnez les éléments probants et choisissez Ajouter au rapport d'évaluation. • Pour exclure des éléments probants, sélectionnez-les et choisissez Supprimer du rapport d'évaluation.

Étapes suivantes

Lorsque vous êtes prêt à explorer les différents éléments de preuve contenus dans un dossier, suivez les étapes décrites dansExamen des preuves dans AWS Audit Manager. Cette page vous guidera à travers les détails des preuves et vous expliquera comment interpréter les informations que vous y voyez.

Ressources supplémentaires

- Pour des solutions aux problèmes liés aux preuves dans Audit Manager, voirRésolution des problèmes liés aux évaluations et à la collecte d'éléments probants.

Examen des preuves dans AWS Audit Manager

Lorsque vous devez examiner un élément de preuve spécifique, suivez les instructions de cette page. Vous trouverez les détails des preuves organisés en plusieurs sections.

Table des matières

Prérequis

La procédure suivante suppose que vous avez déjà créé au moins une évaluation. Si vous n'avez pas encore créé d'évaluation, vous ne verrez aucun résultat si vous suivez ces étapes.

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour consulter une évaluation dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

N'oubliez pas qu'il faut jusqu'à 24 heures pour qu'une évaluation commence à recueillir des preuves automatisées. Si votre évaluation ne contient pas encore de preuves, vous ne verrez aucun résultat si vous suivez ces étapes.

Procédure

Pour ouvrir et consulter une page de détails sur les preuves

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, sélectionnez Évaluations, puis choisissez une évaluation.
3. Sur la page d'évaluation, choisissez l'onglet Contrôles, faites défiler la page vers le bas jusqu'au tableau Contrôles, puis choisissez un contrôle.
4. Sur la page du contrôle, choisissez l'onglet Dossiers d'éléments probants.
5. Dans le tableau Dossiers de preuves, choisissez le nom d'un dossier de preuves.

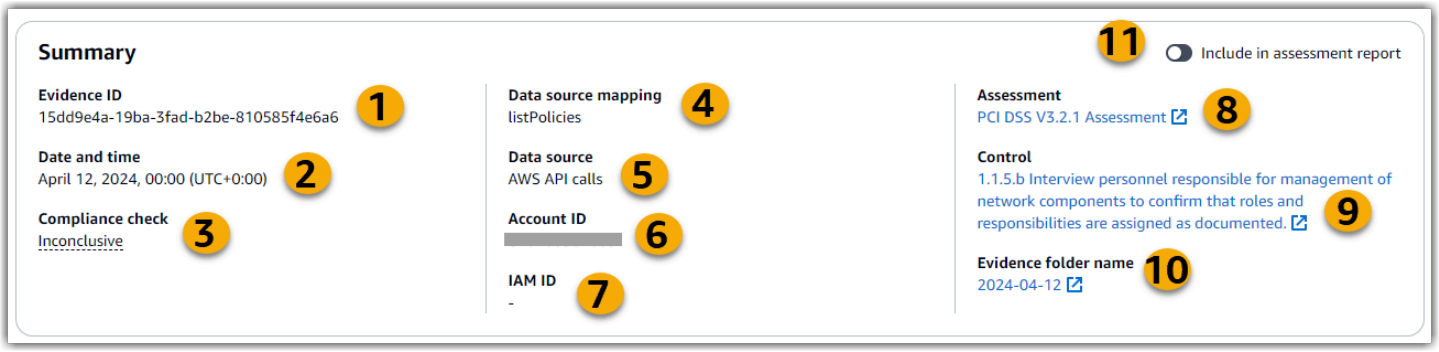
6. Choisissez le nom de la preuve dans la colonne Heure pour ouvrir la page des détails de la preuve.
7. Passez en revue les détails des preuves en utilisant les informations suivantes comme référence.

Sections d'une page de détails sur les preuves

- Récapitulatif
- Attributs
- Ressources incluses

Récapitulatif

Vous pouvez utiliser la section Résumé pour avoir un aperçu des preuves.



Dans cette section, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
1. ID de preuve	L'identifiant unique des preuves.
2. Date et heure	L'heure et la date auxquelles les preuves ont été recueillies. Cela est représenté en temps universel coordonné (UTC).
3. Contrôle de conformité	État de l'évaluation des preuves du contrôle de conformité. • Pour les preuves collectées AWS Security Hub, un résultat de réussite ou d'échec est signalé directement auprès de AWS Security Hub.

Name (Nom)	Description
	• Pour les preuves collectées auprès de AWS Config, un résultat conforme ou non conforme est signalé directement à partir de AWS Config. • Si Non applicable est affiché, cela indique l'une des deux choses suivantes. Soit vous ne l'avez pas fait, AWS Security Hub soit vous l'avez AWS Config activé. Ou bien, les preuves proviennent d'une autre source de données.
4. Cartographie des sources de données	Le mot clé de mappage qui a été utilisé pour collecter les preuves.
5. Data source type (Type de source de données)	Type de source de données à partir de laquelle les preuves ont été collectées.
6. ID de compte	Compte AWS Cela est associé aux preuves.
7. ID IAM	L'utilisateur ou le rôle concerné, le cas échéant.
8. Évaluation	Le nom de l'évaluation associée aux preuves.
9. Contrôle	Le nom du contrôle associé aux preuves.
10. Nom du dossier de preuves	Le nom du dossier de preuves qui contient les preuves.
11. Inclure dans le rapport d'évaluation	Interrupteur qui vous permet d'inclure ou d'exclure les preuves du rapport d'évaluation.

Attributs

Vous pouvez utiliser le tableau des attributs pour voir les attributs des preuves en détail.

Dans ce tableau, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
Nom d'attribut	La clé de l'attribut.

Name (Nom)	Description
Valeur	Valeur de l'attribut. Dans certains cas, un lien vers un fichier JSON est fourni avec des informations supplémentaires.

Ressources incluses

Vous pouvez utiliser le tableau Ressources incluses pour voir les ressources qui ont été évaluées pour générer ces preuves.

Dans cette section, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
ARN	L'Amazon Resource Name (ARN) de la ressource. Un ARN peut ne pas être disponible pour tous les types d'éléments probants.
Conformité des ressources	État de l'évaluation de la ressource. • Pour les preuves collectées AWS Security Hub, un résultat de réussite ou d'échec est signalé directement par Security Hub. • Pour les preuves collectées auprès de AWS Config, un résultat conforme ou non conforme est signalé directement à partir de AWS Config. • Si l'option Non applicable apparaît, cela indique que Security Hub n' AWS Config est pas activé ou que les preuves provienne nt d'une autre source de données.
Valeur	Plus d'informations sur l'évaluation des ressources. Dans certains cas, un lien vers un fichier JSON est fourni avec des informations supplémentaires.

Ressources supplémentaires

- Pour des solutions aux problèmes liés aux preuves dans Audit Manager, voirRésolution des problèmes liés aux évaluations et à la collecte d'éléments probants.

Modifier une évaluation dans AWS Audit Manager

Il se peut que vous deviez modifier vos évaluations existantes dans AWS Audit Manager. La portée de votre audit a peut-être changé, ce qui nécessite des mises à jour de ce qui est Comptes AWS inclus dans l'évaluation. Il se peut également que vous deviez réviser la liste des responsables de l'audit affectés à l'évaluation en raison de changements de personnel. Dans de tels cas, vous pouvez modifier vos évaluations actives et apporter les ajustements nécessaires sans perturber votre collecte de preuves.

La page suivante décrit les étapes à suivre pour modifier les détails de votre évaluation, modifier le Comptes AWS périmètre, informer les responsables de l'audit, vérifier et enregistrer vos modifications.

Prérequis

La procédure suivante suppose que vous avez déjà créé au moins une évaluation et qu'elle est active.

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour modifier une évaluation dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Tâches

- Étape 1 : Modifier les détails de l'évaluation
- Étape 2 : Modifier Comptes AWS dans le champ d'application
- Étape 3 : Modifier les propriétaires de l'audit
- Étape 4 : Vérifiez et enregistrez

Étape 1 : Modifier les détails de l'évaluation

Procédez comme suit pour modifier les détails de votre évaluation.

Pour modifier une évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations.
3. Sélectionnez une évaluation, puis choisissez Modifier.
4. Sous Modifier les détails de l'évaluation, modifiez les détails de votre évaluation selon vos besoins.
5. Choisissez Suivant.

Étape 2 : Modifier Comptes AWS dans le champ d'application

Au cours de cette étape, vous pouvez modifier les comptes inclus dans votre évaluation. Audit Manager peut prendre en charge jusqu'à 200 comptes dans le cadre d'une évaluation.

Pour modifier Comptes AWS dans Scope

1. Pour ajouter un Compte AWS, cochez la case à côté du nom du compte.
2. Pour supprimer un Compte AWS, décochez la case à côté du nom du compte.
3. Choisissez Suivant.

> **Note**
>
> Pour modifier l'administrateur délégué pour Audit Manager, consultezModification d'un administrateur délégué.

Étape 3 : Modifier les propriétaires de l'audit

Au cours de cette étape, vous pouvez modifier les responsables de l'audit inclus dans votre évaluation.

Pour modifier les responsables de l'audit

1. Pour ajouter un responsable de l'audit, cochez la case à côté du nom du compte.
2. Pour supprimer un responsable de l'audit, décochez la case à côté du nom du compte.
3. Choisissez Suivant.

Étape 4 : Vérifiez et enregistrez

Vérifiez les informations de votre évaluation. Pour modifier les informations d'une étape, choisissez Modifier. Lorsque vous avez terminé les modifications, choisissez Enregistrer les modifications pour confirmer vos modifications.

Une fois que vous avez terminé vos modifications, les modifications apportées à l'évaluation prennent effet à 00h00 UTC le jour suivant.

Étapes suivantes

Lorsque vous n'avez plus besoin de collecter des preuves pour un contrôle d'évaluation spécifique, vous pouvez modifier le statut de ce contrôle. Pour obtenir des instructions, veuillez consulter Modification du statut d'un contrôle d'évaluation dans AWS Audit Manager.

Lorsque vous n'avez plus besoin de recueillir des preuves pour l'ensemble de l'évaluation, vous pouvez faire passer le statut de l'évaluation à inactif. Pour obtenir des instructions, veuillez consulter Modification du statut d'une évaluation en inactif dans AWS Audit Manager.

Ressources supplémentaires

- Pour des solutions aux problèmes d'évaluation dans Audit Manager, consultezRésolution des problèmes liés aux évaluations et à la collecte d'éléments probants.
- Pour savoir pourquoi il n'est plus possible de modifier les services concernés, consultez Je ne parviens pas à modifier les services concernés par mon évaluation la section Dépannage de ce guide.

Ajouter des preuves manuelles dans AWS Audit Manager

Audit Manager peut collecter automatiquement des éléments probants pour de nombreux contrôles. Cependant, certains contrôles peuvent nécessiter des preuves qui ne peuvent pas être collectées automatiquement. Dans ce cas, vous pouvez ajouter manuellement vos propres preuves.

Considérez les exemples suivants :

- Certains contrôles concernent la fourniture d'enregistrements physiques (tels que des signatures) ou des événements qui ne sont pas générés dans le cloud (tels que des observations et des

entretiens). Dans ces cas, vous pouvez ajouter manuellement des fichiers à titre de preuve. Par exemple, si un contrôle nécessite des informations sur votre structure organisationnelle, vous pouvez charger une copie de l'organigramme de votre entreprise à titre d'élément probant manuel.

- Certains contrôles constituent une question d'évaluation des risques liés aux fournisseurs. Une question d'évaluation des risques peut nécessiter de la documentation à titre d'élément probant (comme un organigramme). Ou bien, il se peut qu'une simple réponse textuelle (telle qu'une liste des titres de poste) soit nécessaire. Dans ce dernier cas, vous pouvez répondre à la question et enregistrer votre réponse sous forme de preuve manuelle.

Vous pouvez également utiliser la fonctionnalité de chargement manuel pour gérer les éléments probants provenant de plusieurs environnements. Si votre entreprise utilise un modèle de cloud hybride ou multicloud, vous pouvez charger des éléments probants depuis votre environnement sur site, un environnement hébergé dans le cloud ou vos applications SaaS. Cela vous permet d'organiser vos éléments probants (quelle que soit leur provenance) en les stockant dans la structure d'une évaluation d'Audit Manager, où chaque élément probant est associé à un contrôle spécifique.

Points clés

Pour ajouter des preuves manuelles à vos évaluations dans Audit Manager, vous avez le choix entre trois méthodes.

1. Importation d'un fichier depuis Amazon S3 : cette méthode est idéale lorsque des fichiers de preuves sont stockés dans un compartiment S3, tels que de la documentation, des rapports ou d'autres artefacts qui ne peuvent pas être collectés automatiquement par Audit Manager. En important ces fichiers directement depuis S3, vous pouvez intégrer facilement ces preuves manuelles aux preuves collectées automatiquement.
2. Téléchargement d'un fichier depuis votre navigateur : si des fichiers de preuves sont stockés localement sur votre ordinateur ou votre réseau, vous pouvez les télécharger manuellement dans Audit Manager en utilisant cette méthode. Cette approche est particulièrement utile lorsque vous devez inclure des enregistrements physiques, tels que des documents numérisés ou des images, qui ne sont pas disponibles au format numérique dans votre AWS environnement.
3. Ajouter du texte libre comme preuve - Dans certains cas, les preuves que vous devez fournir ne prennent pas la forme d'un fichier, mais plutôt d'une réponse ou d'une explication textuelle. Cette méthode vous permet de saisir du texte en format libre directement dans Audit Manager. Cela peut être particulièrement utile lorsque vous répondez aux questions d'évaluation des risques des fournisseurs.

Ressources supplémentaires

- Pour obtenir des instructions sur la façon d'ajouter des preuves manuelles à un contrôle d'évaluation, consultez les ressources suivantes. N'oubliez pas que vous ne pouvez utiliser qu'une seule méthode à la fois.
  - Importation de fichiers de preuves manuels depuis Amazon S3
  - Téléchargement manuel de fichiers de preuves depuis votre navigateur
  - Saisir des réponses sous forme de texte libre comme preuve manuelle
- Pour savoir quels formats de fichier vous pouvez utiliser, consultezFormats de fichier pris en charge pour les éléments probants manuels.
- Pour en savoir plus sur les différents types de preuves dans Audit Manager, consultez evidence la section Concepts et terminologie de ce guide.
- Pour obtenir de l'aide au dépannage, consultezJe ne parviens pas à charger des éléments probants manuels dans un contrôle.

Importation de fichiers de preuves manuels depuis Amazon S3

Vous pouvez importer manuellement des fichiers de preuves depuis un compartiment Amazon S3 dans votre évaluation. Cela vous permet de compléter les preuves collectées automatiquement par des pièces justificatives supplémentaires.

Prérequis

- La taille maximale prise en charge pour un seul fichier d'élément probant manuel est de 100 Mo.
- Vous devez utiliser l'un desFormats de fichier pris en charge pour les éléments probants manuels.
- Chacun Compte AWS peut télécharger manuellement jusqu'à 100 fichiers de preuves vers un contrôle chaque jour. Le dépassement de ce quota quotidien entraîne l'échec de tout chargement manuel supplémentaire pour le contrôle en question. Si vous devez charger une grande quantité d'éléments probants manuels dans un seul contrôle, chargez-les par lots sur plusieurs jours.
- Lorsqu'un contrôle est inactif, vous ne pouvez pas charger d'éléments probants manuels pour ce contrôle. Pour ajouter des preuves manuelles, vous devez d'abord modifier le statut du contrôle en cours de révision ou en cours de révision.
- Assurez-vous que votre identité IAM dispose des autorisations appropriées pour gérer une évaluation dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces

autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Vous pouvez importer un fichier à l'aide de la console Audit Manager, de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

AWS console

Pour importer un fichier depuis S3 sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, sélectionnez Évaluations, puis choisissez une évaluation.
3. Choisissez l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'à Ensembles de contrôles, puis choisissez un contrôle.
4. Dans l'onglet Dossiers d'éléments probants, choisissez Ajouter des éléments probants manuels, puis choisissez Importer un fichier depuis S3.
5. Sur la page suivante, saisissez l'URI S3 des éléments probants. Vous pouvez trouver l'URI S3 en accédant à l'objet dans la console Amazon S3 et en choisissant Copy S3 URI.
6. Sélectionnez Charger.

AWS CLI

Dans la procédure suivante, remplacez le *texte de l'espace réservé* par vos propres informations.

Pour importer un fichier depuis S3 dans le AWS CLI

1. Exécutez la commande `list-assessments` pour afficher la liste de vos évaluations.

```
aws auditmanager list-assessments
```

Dans la réponse, recherchez l'évaluation dans laquelle vous souhaitez charger des éléments probants et notez l'identifiant de l'évaluation.

2. Exécutez la commande `get-assessment` et spécifiez l'ID d'évaluation indiqué à la première étape.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

Dans la réponse, recherchez l'ensemble de contrôles et le contrôle vers lesquels vous souhaitez charger des éléments probants, et notez leurs identifiants.

3. Exécutez la commande `batch-import-evidence-to-assessment-control` avec les paramètres suivants :

- `--assessment-id`— Utilisez l'identifiant d'évaluation indiqué à l'étape 1.
- `--control-set-id`— Utilisez l'identifiant de l'ensemble de contrôles indiqué à l'étape 2.
- `--control-id`— Utilisez l'identifiant de contrôle indiqué à l'étape 2.
- `--manual-evidence`— Utilisez `s3ResourcePath` comme type d'élément probant manuel et spécifiez l'URI S3 de l'élément probant. Vous pouvez trouver l'URI S3 en accédant à l'objet dans la console Amazon S3 et en choisissant Copy S3 URI.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence s3ResourcePath=s3://
DOC-EXAMPLE-BUCKET/EXAMPLE-FILE.extension
```

Audit Manager API

Pour importer un fichier depuis S3 à l'aide de l'API

1. Appelez l'opération `ListAssessments` pour obtenir la liste de vos évaluations. Dans la réponse, recherchez l'évaluation dans laquelle vous souhaitez charger des éléments probants et notez l'identifiant de l'évaluation.
2. Appelez l'opération `GetAssessment` et spécifiez l'identifiant d'évaluation indiqué à la première étape. Dans la réponse, recherchez l'ensemble de contrôles et le contrôle vers lesquels vous souhaitez charger des éléments probants, et notez leurs identifiants.
3. Appelez l'opération `BatchImportEvidenceToAssessmentControl` avec les paramètres suivants :

- `assessmentId`— Utilisez l'identifiant d'évaluation indiqué à l'étape 1.
- `controlSetId`— Utilisez l'identifiant de l'ensemble de contrôles indiqué à l'étape 2.
- `controlId`— Utilisez l'identifiant de contrôle indiqué à l'étape 2.
- `manualEvidence`— Utilisez `s3ResourcePath` comme type d'élément probant manuel et spécifiez l'URI S3 de l'élément probant. Vous pouvez trouver l'URI S3 en accédant à l'objet dans la console Amazon S3 et en choisissant Copy S3 URI.

Pour plus d'informations, choisissez l'un des liens de la procédure précédente pour en savoir plus dans la référence de l'AWS Audit Manager API. Cela inclut des informations sur la façon d'utiliser ces opérations et paramètres dans l'un des SDK spécifiques au langage AWS .

Étapes suivantes

Après avoir ajouté et examiné les preuves de votre évaluation, vous pouvez générer un rapport d'évaluation. Pour plus d'informations, consultez Préparation d'un rapport d'évaluation dans AWS Audit Manager.

Ressources supplémentaires

Pour savoir quels formats de fichier vous pouvez utiliser, consultezFormats de fichier pris en charge pour les éléments probants manuels.

Téléchargement manuel de fichiers de preuves depuis votre navigateur

Vous pouvez télécharger manuellement des fichiers de preuves depuis votre navigateur dans votre évaluation Audit Manager. Cela vous permet de compléter les preuves collectées automatiquement par des pièces justificatives supplémentaires.

Prérequis

- La taille maximale prise en charge pour un seul fichier d'élément probant manuel est de 100 Mo.
- Vous devez utiliser l'un desFormats de fichier pris en charge pour les éléments probants manuels.
- Chacun Compte AWS peut télécharger manuellement jusqu'à 100 fichiers de preuves vers un contrôle chaque jour. Le dépassement de ce quota quotidien entraîne l'échec de tout chargement manuel supplémentaire pour le contrôle en question. Si vous devez charger une grande quantité d'éléments probants manuels dans un seul contrôle, chargez-les par lots sur plusieurs jours.

- Lorsqu'un contrôle est inactif, vous ne pouvez pas charger d'éléments probants manuels pour ce contrôle. Pour ajouter des preuves manuelles, vous devez d'abord modifier le statut du contrôle en cours de révision ou en cours de révision.
- Assurez-vous que votre identité IAM dispose des autorisations appropriées pour gérer une évaluation dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Vous pouvez télécharger un fichier à l'aide de la console Audit Manager, de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

AWS console

Pour télécharger un fichier depuis votre navigateur sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, sélectionnez Évaluations, puis choisissez une évaluation.
3. Dans l'onglet Contrôles, faites défiler l'écran jusqu'à Ensembles de contrôles, puis choisissez un contrôle.
4. Dans l'onglet Dossiers de preuves, choisissez Ajouter des preuves manuelles.
5. Choisissez Charger le fichier depuis le navigateur.
6. Choisissez le dossier que vous souhaitez charger.
7. Sélectionnez Charger.

AWS CLI

Dans la procédure suivante, remplacez le *texte de l'espace réservé* par vos propres informations.

Pour télécharger un fichier depuis votre navigateur dans le AWS CLI

1. Exécutez la commande `list-assessments` pour afficher la liste de vos évaluations.

```
aws auditmanager list-assessments
```

Dans la réponse, recherchez l'évaluation dans laquelle vous souhaitez charger des éléments probants et notez l'identifiant de l'évaluation.

2. Exécutez la commande `get-assessment` et spécifiez l'ID d'évaluation indiqué à la première étape.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

Dans la réponse, recherchez l'ensemble de contrôles et le contrôle vers lesquels vous souhaitez charger des éléments probants, et notez leurs identifiants.

3. Exécutez la commande`get-evidence-file-upload-url` et spécifiez le fichier que vous voulez charger.

```
aws auditmanager get-evidence-file-upload-url --file-name fileName.extension
```

Dans la réponse, prenez note de l'URL présignée et du `evidenceFileName`.

4. Utilisez l'URL présignée de la troisième étape pour charger le fichier depuis votre navigateur. Cette action charge votre fichier sur Amazon S3, où il est enregistré en tant qu'objet pouvant être joint à un contrôle d'évaluation. Dans l'étape suivante, vous allez référencer l'objet nouvellement créé à l'aide du paramètre `evidenceFileName`.

> **Note**
>
> Lorsque vous chargez un fichier à l'aide d'une URL présignée, Audit Manager protège et stocke vos données en utilisant le chiffrement côté serveur avec AWS Key Management Service. À cette fin, vous devez utiliser l'en-tête `x-amz-server-side-encryption` de votre demande lorsque vous utilisez l'URL présignée pour charger votre fichier.
> Si vous utilisez un client géré AWS KMS key dans les Configuration de vos paramètres de chiffrement des données paramètres de votre Audit Manager, assurez-vous d'inclure également l'`x-amz-server-side-encryption-aws-kms-key-id`en-tête dans votre demande. Si l'en-tête `x-amz-server-side-`

`encryption-aws-kms-key-id` n'est pas présent dans la demande, Amazon S3 suppose que vous souhaitez utiliser la Clé gérée par AWS.
Pour plus d'informations, consultez la section Protection des données à l'aide du chiffrement côté serveur à l'aide de AWS Key Management Service clés (SSE-KMS) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

5. Exécutez la commande `batch-import-evidence-to-assessment-control` avec les paramètres suivants :

   - `--assessment-id`— Utilisez l'identifiant d'évaluation indiqué à l'étape 1.
   - `--control-set-id`— Utilisez l'identifiant de l'ensemble de contrôles indiqué à l'étape 2.
   - `--control-id`— Utilisez l'identifiant de contrôle indiqué à l'étape 2.
   - `--manual-evidence`— Utilisez `evidenceFileName` comme type d'élément probant manuel et spécifiez le nom du fichier d'éléments probants à l'étape 3.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet
 --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence
 evidenceFileName=fileName.extension
```

Audit Manager API

Pour télécharger un fichier depuis votre navigateur à l'aide de l'API

1. Appelez l'opération `ListAssessments`. Dans la réponse, recherchez l'évaluation dans laquelle vous souhaitez charger des éléments probants et notez l'identifiant de l'évaluation.
2. Appelez l'opération `GetAssessment` et spécifiez la `assessmentId` à partir de la première étape. Dans la réponse, recherchez l'ensemble de contrôles et le contrôle vers lesquels vous souhaitez charger des éléments probants, et notez leurs identifiants.
3. Appelez l'opération `GetEvidenceFileUploadUrl` et précisez le fichier `fileName` que vous souhaitez charger. Dans la réponse, prenez note de l'URL présignée et du `evidenceFileName`.
4. Utilisez l'URL présignée de la troisième étape pour charger le fichier depuis votre navigateur. Cette action charge votre fichier sur Amazon S3, où il est enregistré en tant qu'objet pouvant

être joint à un contrôle d'évaluation. Dans l'étape suivante, vous allez référencer l'objet nouvellement créé à l'aide du paramètre `evidenceFileName`.

> **Note**
>
> Lorsque vous chargez un fichier à l'aide d'une URL présignée, Audit Manager protège et stocke vos données en utilisant le chiffrement côté serveur avec AWS Key Management Service. À cette fin, vous devez utiliser l'en-tête `x-amz-server-side-encryption` de votre demande lorsque vous utilisez l'URL présignée pour charger votre fichier.
>
> Si vous utilisez un client géré AWS KMS key dans les Configuration de vos paramètres de chiffrement des données paramètres de votre Audit Manager, assurez-vous d'inclure également l'`x-amz-server-side-encryption-aws-kms-key-id`en-tête dans votre demande. Si l'en-tête `x-amz-server-side-encryption-aws-kms-key-id` n'est pas présent dans la demande, Amazon S3 suppose que vous souhaitez utiliser la Clé gérée par AWS.
>
> Pour plus d'informations, consultez la section Protection des données à l'aide du chiffrement côté serveur à l'aide de AWS Key Management Service clés (SSE-KMS) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

5. Appelez l'opération `BatchImportEvidenceToAssessmentControl` avec les paramètres suivants :

   - `assessmentId`— Utilisez l'identifiant d'évaluation indiqué à l'étape 1.
   - `controlSetId`— Utilisez l'identifiant de l'ensemble de contrôles indiqué à l'étape 2.
   - `controlId`— Utilisez l'identifiant de contrôle indiqué à l'étape 2.
   - `manualEvidence`— Utilisez `evidenceFileName` comme type d'élément probant manuel et spécifiez le nom du fichier d'éléments probants à l'étape 3.

Pour plus d'informations, choisissez l'un des liens de la procédure précédente pour en savoir plus dans la référence de l'AWS Audit Manager API. Cela inclut des informations sur la façon d'utiliser ces opérations et paramètres dans l'un des SDK spécifiques au langage AWS .

Étapes suivantes

Après avoir collecté et examiné les preuves de votre évaluation, vous pouvez générer un rapport d'évaluation. Pour plus d'informations, consultez Préparation d'un rapport d'évaluation dans AWS Audit Manager.

Ressources supplémentaires

Pour savoir quels formats de fichier vous pouvez utiliser, consultezFormats de fichier pris en charge pour les éléments probants manuels.

Saisir des réponses sous forme de texte libre comme preuve manuelle

Vous pouvez fournir un contexte supplémentaire et des informations complémentaires pour un contrôle d'évaluation en saisissant du texte libre et en enregistrant ce texte comme preuve. Cela vous permet de documenter manuellement les détails qui ne sont pas capturés par le biais de la collecte automatique de preuves.

Par exemple, vous pouvez utiliser Audit Manager pour créer des contrôles personnalisés représentant les questions d'un questionnaire d'évaluation des risques liés aux fournisseurs. Dans ce cas, le nom de chaque contrôle est une question spécifique qui demande des informations sur le niveau de sécurité et de conformité de votre organisation. Pour enregistrer votre réponse à une question d'évaluation des risques fournisseurs donnée, vous pouvez saisir une réponse textuelle et l'enregistrer comme preuve manuelle pour le contrôle.

Prérequis

- Lorsqu'un contrôle est inactif, vous ne pouvez pas charger d'éléments probants manuels pour ce contrôle. Pour ajouter des preuves manuelles, vous devez d'abord modifier le statut du contrôle en cours de révision ou en cours de révision.
- Assurez-vous que votre identité IAM dispose des autorisations appropriées pour gérer une évaluation dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Vous pouvez saisir des réponses textuelles à l'aide de la console Audit Manager, de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

AWS console

Pour saisir une réponse textuelle sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, sélectionnez Évaluations, puis choisissez une évaluation.
3. Choisissez l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'à Ensembles de contrôles, puis choisissez un contrôle.
4. Dans l'onglet Dossiers de preuves, choisissez Ajouter des preuves manuelles.
5. Choisissez Entrer une réponse textuelle.
6. Dans la fenêtre contextuelle qui apparaît, saisissez votre réponse en texte brut.
7. Choisissez Confirmer.

AWS CLI

Dans la procédure suivante, remplacez le *texte de l'espace réservé* par vos propres informations.

Pour saisir une réponse textuelle dans le AWS CLI

1. Exécutez la commande `list-assessments`.

   ```
   aws auditmanager list-assessments
   ```

   Dans la réponse, recherchez l'évaluation dans laquelle vous souhaitez charger des éléments probants et notez l'identifiant de l'évaluation.
2. Exécutez la commande `get-assessment` et spécifiez l'ID d'évaluation indiqué à la première étape.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

Dans la réponse, recherchez l'ensemble de contrôles et le contrôle vers lesquels vous souhaitez charger des éléments probants, et notez leurs identifiants.

3. Exécutez la commande batch-import-evidence-to-assessment-control avec les paramètres suivants :

   - `--assessment-id`— Utilisez l'identifiant d'évaluation indiqué à l'étape 1.
   - `--control-set-id`— Utilisez l'identifiant de l'ensemble de contrôles indiqué à l'étape 2.
   - `--control-id`— Utilisez l'identifiant de contrôle indiqué à l'étape 2.
   - `--manual-evidence`— `textResponse` Utilisez-le comme type d'élément probant manuel et entrez le texte que vous souhaitez enregistrer en tant qu'élément probant manuel.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence textResponse="enter
 text here"
```

Audit Manager API

Pour saisir une réponse textuelle à l'aide de l'API

1. Appelez l'opération ListAssessments. Dans la réponse, recherchez l'évaluation dans laquelle vous souhaitez charger des éléments probants et notez l'identifiant de l'évaluation.
2. Appelez l'opération GetAssessment et spécifiez la `assessmentId` à partir de la première étape. Dans la réponse, recherchez l'ensemble de contrôles et le contrôle vers lesquels vous souhaitez charger des éléments probants, et notez leurs identifiants.
3. Appelez l'opération BatchImportEvidenceToAssessmentControl avec les paramètres suivants :

   - assessmentId— Utilisez l'identifiant d'évaluation indiqué à l'étape 1.
   - controlSetId— Utilisez l'identifiant de l'ensemble de contrôles indiqué à l'étape 2.

- `controlId`— Utilisez l'identifiant de contrôle indiqué à l'étape 2.
- `manualEvidence`— `textResponse` Utilisez-le comme type d'élément probant manuel et entrez le texte que vous souhaitez enregistrer en tant qu'élément probant manuel.

Pour plus d'informations, choisissez l'un des liens de la procédure précédente pour en savoir plus dans la référence de l'AWS Audit Manager API. Cela inclut des informations sur la façon d'utiliser ces opérations et paramètres dans l'un des SDK spécifiques au langage AWS .

Étapes suivantes

Après avoir collecté et examiné les preuves de votre évaluation, vous pouvez générer un rapport d'évaluation. Pour plus d'informations, consultez Préparation d'un rapport d'évaluation dans AWS Audit Manager.

Formats de fichier pris en charge pour les éléments probants manuels

Le tableau ci-dessous répertorie et décrit les types de fichiers que vous pouvez charger à titre d'élément probant manuel. Pour chaque type de fichier, le tableau répertorie également les extensions de fichier prises en charge.

Type de fichier	Description	Extensions de fichier prises en charge
Compression ou archivage	Archives compressé es GNU et archives compressées ZIP	`.gz`, `.zip`
Document	Fichiers de documents courants tels que les PDF et les fichiers Microsoft Office	`.doc`, `.docx`, `.pdf`, `.ppt`, `.pptx`, `.xls`, `.xlsx`
Image	Fichiers d'images et de graphiques	`.jpeg`, `.jpg`, `.png`, `.svg`
Texte	Autres fichiers texte non binaires, tels que les documents en texte brut et	`.cer`, `.csv`, `.html`, `.jmx`, `.json`, `.md`, `.out`, `.rtf`, `.txt`, `.xml`, `.yaml`, `.yml`

Type de fichier	Description	Extensions de fichier prises en charge
	les fichiers de langage de balisage	

Ressources supplémentaires

Consultez les pages suivantes pour découvrir les différentes manières d'ajouter vos propres preuves à un contrôle d'évaluation.

- Importation de fichiers de preuves manuels depuis Amazon S3
- Téléchargement manuel de fichiers de preuves depuis votre navigateur
- Saisir des réponses sous forme de texte libre comme preuve manuelle

Préparation d'un rapport d'évaluation dans AWS Audit Manager

Après avoir collecté et examiné les preuves de votre évaluation, vous pouvez générer un rapport d'évaluation. Un rapport d'évaluation résume votre évaluation et fournit des liens vers un ensemble organisé de dossiers contenant les preuves associées.

Points clés

Les preuves nouvellement recueillies n'apparaissent pas automatiquement dans un rapport d'évaluation. Cela signifie que vous pouvez contrôler les preuves que vous souhaitez inclure dans le rapport. Après avoir sélectionné les preuves que vous souhaitez inclure, vous pouvez générer le rapport d'évaluation final à partager avec vos auditeurs.

Lorsque vous générez un rapport d'évaluation, il est placé dans le compartiment S3 que vous avez choisi comme destination du rapport d'évaluation. Vous pouvez également télécharger le rapport d'évaluation depuis le centre de téléchargement d'Audit Manager.

Ressources supplémentaires

Pour plus d'informations sur les rapports d'évaluation et sur la façon de les gérer, consultez les ressources suivantes.

- Ajouter des éléments probants à un rapport d'évaluation

- Supprimer des éléments probants d'un rapport d'évaluation
- Génération de rapports d'évaluation
- Téléchargement d'un rapport d'évaluation
- Navigation dans un rapport d'évaluation et exploration de son contenu
- Validation d'un rapport d'évaluation
- Suppression d'un rapport d'évaluation
- Génération de rapports d'évaluation à partir des résultats de recherche de votre outil de recherche de preuves
- Configuration de la destination par défaut de votre rapport d'évaluation
- Résolution des problèmes liés aux rapports d'évaluation

Ajouter des éléments probants à un rapport d'évaluation

Avant de pouvoir générer un rapport d'évaluation, vous devez ajouter au moins un élément probant à votre rapport d'évaluation. Vous pouvez soit ajouter un dossier de preuves complet, soit ajouter des éléments de preuve spécifiques à partir d'un dossier.

Procédure

Pour inclure des preuves dans un rapport d'évaluation, procédez comme suit.

Ajouter des éléments probants à un rapport d'évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, sélectionnez Évaluations, puis choisissez une évaluation.
3. Dans l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'au tableau des ensembles de contrôles et choisissez un contrôle contenant des preuves que vous souhaitez inclure dans le rapport d'évaluation.
4. Choisissez comment ajouter des éléments probants à votre rapport d'évaluation.

    a. Pour ajouter un dossier d'éléments probants complet, faites défiler l'écran vers le bas jusqu'à Dossiers d'éléments probants, sélectionnez le dossier que vous souhaitez ajouter, puis choisissez Ajouter au rapport d'évaluation.

> **Tip**
>
> Si le dossier que vous recherchez ne s'affiche pas, définissez le filtre déroulant sur Toutes les dates. Dans le cas contraire, les dossiers des sept derniers jours s'afficheront par défaut.
> Si Ajouter au rapport d'évaluation est grisé, le dossier d'éléments probants a déjà été ajouté au rapport d'évaluation.

b. Pour ajouter des éléments probants spécifiques, choisissez un dossier d'éléments probants pour ouvrir son contenu. Sélectionnez un ou plusieurs éléments dans la liste, puis choisissez Ajouter au rapport d'évaluation.

> **Tip**
>
> Si Ajouter au rapport d'évaluation est grisé, assurez-vous d'avoir coché la case à côté des éléments probants, puis réessayez.

5. Une fois que vous avez ajouté les éléments probants au rapport d'évaluation, un bandeau vert de réussite apparaît. Choisissez Afficher les éléments probants dans le rapport d'évaluation pour voir les éléments probants qui seront inclus dans votre rapport d'évaluation.
   - Vous pouvez également consulter les éléments probants qui seront inclus dans votre rapport d'évaluation en revenant à votre évaluation et en choisissant l'onglet de sélection du rapport d'évaluation.

Étapes suivantes

Si vous devez supprimer des preuves d'un rapport d'évaluation, consultezSupprimer des éléments probants d'un rapport d'évaluation.

Lorsque vous êtes prêt à générer un rapport d'évaluation, consultezGénération de rapports d'évaluation.

Ressources supplémentaires

Pour trouver des réponses aux questions et problèmes courants, consultez Résolution des problèmes liés aux rapports d'évaluation la section Dépannage de ce guide.

Supprimer des éléments probants d'un rapport d'évaluation

Si vous devez supprimer des éléments probants d'un rapport d'évaluation, procédez comme suit. Vous pouvez soit supprimer un dossier d'éléments probants complet, soit supprimer des éléments probants individuels à partir d'un dossier.

Procédure

Pour supprimer des éléments probants d'un rapport d'évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations, puis sélectionnez le nom d'une évaluation pour l'ouvrir.
3. Dans l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'au tableau des Ensembles de contrôles et choisissez le nom d'un contrôle pour l'ouvrir.
4. Choisissez la manière dont vous souhaitez supprimer des éléments probants de votre rapport d'évaluation.

   a. Pour supprimer un dossier d'éléments probants complet, faites défiler l'écran vers le bas jusqu'à Dossiers d'éléments probants, sélectionnez le dossier que vous souhaitez supprimer, puis choisissez Supprimer du rapport d'évaluation.

   > **Tip**
   >
   > Si le dossier que vous recherchez ne s'affiche pas, définissez le filtre déroulant sur Toutes les dates. Dans le cas contraire, les dossiers des sept derniers jours s'afficheront par défaut.
   > Si Ajouter au rapport d'évaluation est grisé, le dossier d'éléments probants a déjà été supprimé du rapport d'évaluation.

   b. Pour supprimer des éléments probants spécifiques, choisissez un dossier d'éléments probants pour ouvrir son contenu. Sélectionnez un ou plusieurs éléments dans la liste, puis choisissez Supprimer du rapport d'évaluation.

> **Tip**
>
> Si Supprimer du rapport d'évaluation est grisé, assurez-vous d'avoir coché la case à côté des éléments probants, puis réessayez.

5. Une fois que vous avez ajouté les éléments probants au rapport d'évaluation, un bandeau vert de réussite apparaît. Choisissez Afficher les éléments probants dans le rapport d'évaluation pour voir les éléments probants qui seront inclus dans votre rapport d'évaluation.
   - Vous pouvez également consulter les éléments probants qui seront inclus dans votre rapport d'évaluation en revenant à votre évaluation et en choisissant l'onglet de sélection du rapport d'évaluation.

Étapes suivantes

Lorsque vous êtes prêt à générer un rapport d'évaluation, consultezGénération de rapports d'évaluation.

Ressources supplémentaires

Pour trouver des réponses aux questions et problèmes courants, consultez Résolution des problèmes liés aux rapports d'évaluation la section Dépannage de ce guide.

Génération de rapports d'évaluation

Lorsque vous êtes prêt à générer votre rapport d'évaluation, procédez comme suit.

Prérequis

Avant de pouvoir générer un rapport d'évaluation, vous devez ajouter au moins un élément probant à votre rapport d'évaluation. Vous pouvez soit ajouter un dossier d'éléments probants complet, soit ajouter des éléments probants individuels à partir d'un dossier.

Pour vous assurer que votre rapport d'évaluation est correctement généré, consultez notre Conseils de configuration pour la destination de votre rapport d'évaluation.

Procédure

Pour générer un rapport d'évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation de gauche, sélectionnez Évaluations.
3. Choisissez le nom de l'évaluation pour laquelle générer un rapport d'évaluation.
4. Choisissez l'onglet de Sélection du rapport d'évaluation, puis sélectionnez Générer le rapport d'évaluation.

   > **Tip**
   >
   > Si l'option Générer un rapport d'évaluation est grisée, cela signifie qu'aucun élément probant n'a encore été ajouté au rapport d'évaluation.

5. Dans la fenêtre contextuelle, saisissez le nom et la description du rapport d'évaluation, puis passez en revue les détails du rapport d'évaluation.
6. Choisissez Générer un rapport d'évaluation et attendez quelques minutes pendant que votre rapport d'évaluation est généré.
7. Recherchez et chargez votre rapport d'évaluation depuis la page du Centre de téléchargement de la console Audit Manager.
   - Vous pouvez également accéder au compartiment S3 de destination de votre rapport d'évaluation et charger le rapport d'évaluation à partir de là.

Étapes suivantes

Une fois que vous aurez généré un rapport d'évaluation, vous pourrez approfondir vos connaissances en vue de :

- Trouver et charger votre rapport d'évaluation : découvrir comment charger votre rapport d'évaluation depuis le centre de téléchargement ou depuis Amazon S3.
- Explorer votre rapport d'évaluation : découvrir comment naviguer dans un rapport d'évaluation et explorer son contenu.
- Validez votre rapport d'évaluation : découvrez comment utiliser le fonctionnement de l'ValidateAssessmentReportIntegrityAPI pour valider votre rapport d'évaluation.

- Supprimer un rapport d'évaluation indésirable : découvrir comment supprimer un rapport indésirable du centre de téléchargement ou d'Amazon S3.
- Générez des rapports d'évaluation à partir de l'outil de recherche de preuves — Découvrez comment générer des rapports d'évaluation à partir des résultats de recherche de votre outil de recherche de preuves.

Ressources supplémentaires

Pour trouver des réponses aux questions et problèmes courants, consultez Résolution des problèmes liés aux rapports d'évaluation la section Dépannage de ce guide.

Modification du statut d'un contrôle d'évaluation dans AWS Audit Manager

Vous pouvez modifier le statut d'un contrôle d'évaluation dans votre évaluation active. La mise à jour du statut d'un contrôle vous permet de suivre sa progression et d'indiquer quand vous l'avez revu, afin de garder votre évaluation organisée et up-to-date.

Prérequis

La procédure suivante suppose que vous avez déjà créé une évaluation et que son statut actuel est actif.

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour gérer une évaluation dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Vous pouvez mettre à jour le statut d'un contrôle d'évaluation à l'aide de la console Audit Manager, de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

> **Note**
>
> La modification du statut d'un contrôle en Vérifié est définitive. Une fois que vous avez défini le statut d'un contrôle sur Vérifié, vous ne pouvez plus modifier le statut de ce contrôle ni revenir à un statut précédent.

Audit Manager console

Pour modifier le statut d'un contrôle d'évaluation sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations.
3. Choisissez le nom de l'évaluation pour l'ouvrir.
4. Sur la page d'évaluation, choisissez l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'au tableau des Ensembles de contrôles, puis choisissez le nom d'un contrôle pour l'ouvrir.
5. Choisissez Mettre à jour le statut du contrôle en haut à droite de la page, puis choisissez un statut :

État	Description
En cours de révision	Choisissez ce statut si vous n'avez pas encore revu le contrôle.
Révisé	Choisissez ce statut si vous avez terminé d'examiner les preuves de ce contrôle et que vous souhaitez continuer à collecter ou à ajouter des preuves.
Inactif	Choisissez ce statut si vous souhaitez arrêter de collecter des preuves automatisées pour ce contrôle.

6. Choisissez Mettre à jour le statut du contrôle pour confirmer votre choix.

AWS CLI

Pour modifier le statut d'un contrôle d'évaluation dans AWS CLI

1. Exécutez la commande list-assessment.

```
aws auditmanager list-assessments
```

La réponse renvoie une liste d'évaluations. Recherchez l'évaluation qui contient le contrôle que vous souhaitez mettre à jour et prenez note de l'identifiant de l'évaluation.

2. Exécutez la commande get-assessment et spécifiez l'ID d'évaluation indiqué à l'étape 1.

Dans l'exemple suivant, remplacez le *texte de l'espace réservé* par vos propres informations.

```
 aws auditmanager get-assessment --assessment-
id 1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4e5f6g
```

Dans la réponse, recherchez le contrôle que vous souhaitez mettre à jour et prenez note de l'ID du contrôle et de son ID d'ensemble de contrôles.

3. Exécutez la update-assessment-controlcommande et spécifiez les paramètres suivants :

- `--assessment-id`— L'évaluation à laquelle appartient le contrôle.
- `--control-set-id`— Le jeu de commandes auquel appartient le contrôle.
- `--control-id`— Le contrôle que vous souhaitez mettre à jour.
- `--control-status`— Définissez cette valeur sur `UNDER_REVIEWREVIEWED`, ou`INACTIVE`.

Dans l'exemple suivant, remplacez le *texte de l'espace réservé* par vos propres informations.

```
aws auditmanager update-assessment-control --assessment-
id 1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4e5f6g --control-set-id "My control set" --
control-id 2b3c4d5e-2b3c-2b3c-2b3c-2b3c4d5f6g7h --control-status REVIEWED
```

Audit Manager API

Pour modifier le statut d'un contrôle d'évaluation à l'aide de l'API

1. Utilisez l'ListAssessmentsopération.

   Dans la réponse, recherchez l'évaluation contenant le contrôle que vous souhaitez mettre à jour et notez l'identifiant de l'évaluation.
2. Utilisez l'GetAssessmentopération et spécifiez l'ID d'évaluation indiqué à l'étape 1.

   Dans la réponse, recherchez le contrôle que vous souhaitez mettre à jour et prenez note de l'ID du contrôle et de son ID d'ensemble de contrôles.
3. Utilisez l'UpdateAssessmentControlopération et spécifiez les paramètres suivants :

   - `assessmentId`— L'évaluation à laquelle appartient le contrôle.
   - `controlSetId`— Le jeu de commandes auquel appartient le contrôle.
   - `controlId`: le contrôle que vous souhaitez mettre à jour.
   - `controlStatus`— Définissez cette valeur sur `UNDER_REVIEWREVIEWED`, ou`INACTIVE`.

Pour plus d'informations sur ces opérations d'API, cliquez sur l'un des liens de la procédure précédente pour en savoir plus dans la référence des AWS Audit Manager API. Cela inclut des informations sur la façon d'utiliser ces opérations et paramètres dans l'un des SDK spécifiques au langage AWS .

Étapes suivantes

Lorsque vous êtes prêt à modifier le statut de l'évaluation, consultezModification du statut d'une évaluation en inactif dans AWS Audit Manager.

Modification du statut d'une évaluation en inactif dans AWS Audit Manager

Lorsque vous n'avez plus besoin de collecter des preuves pour une évaluation, vous pouvez modifier son statut en le configurant sur Inactif. Lorsque le statut d'une évaluation est configuré sur inactif, celle-ci cesse de collecter des preuves. Par conséquent, vous ne payez plus de frais pour cette évaluation.

Outre l'arrêt de la collecte d'éléments probants, Audit Manager apporte les modifications suivantes aux contrôles inclus dans l'évaluation inactive :

- Tous les ensembles de contrôles passent au statut Vérifié.
- Tous les contrôles En cours de vérification passent au statut Vérifié.
- Les délégués chargés de l'évaluation inactive ne peuvent plus consulter ni modifier ses contrôles et ses ensembles de contrôles.

Prérequis

La procédure suivante suppose que vous avez déjà créé une évaluation et que son statut actuel est actif.

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour gérer une évaluation dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Vous pouvez mettre à jour le statut d'une évaluation à l'aide de la console Audit Manager, de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

> **Warning**
>
> Cette action est irréversible. Nous vous recommandons de procéder avec prudence et de vous assurer que vous souhaitez définir votre évaluation comme étant inactif. Lorsqu'une évaluation est inactive, vous disposez d'un accès en lecture seule à son contenu. Cela signifie que vous pouvez toujours examiner les preuves précédemment collectées et générer des rapports d'évaluation. Cependant, vous ne pouvez pas modifier l'évaluation inactive, ajouter des commentaires ou charger des preuves manuelles.

Audit Manager console

Pour modifier le statut d'une évaluation en inactif sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.

2. Dans le volet de navigation, choisissez Évaluations.
3. Choisissez le nom de l'évaluation pour l'ouvrir.
4. En haut à droite de la page, choisissez Mettre à jour le statut de l'évaluation, puis sélectionnez Inactif.
5. Choisissez Mettre à jour le statut dans la fenêtre contextuelle pour confirmer que vous souhaitez changer le statut en inactif.

Les modifications apportées à l'évaluation et à ses contrôles prennent effet au bout d'une minute environ.

AWS CLI

Pour faire passer le statut d'une évaluation à inactif dans AWS CLI

1. Tout d'abord, identifiez l'évaluation que vous voulez mettre à jour. Pour ce faire, exécutez la commande list-assessments.

```
aws auditmanager list-assessments
```

La réponse renvoie une liste d'évaluations. Recherchez l'évaluation que vous souhaitez désactiver et prenez note de l'identifiant de l'évaluation.

2. Ensuite, exécutez la update-assessment-statuscommande et spécifiez les paramètres suivants :

- `--assessment-id`— Utilisez ce paramètre pour spécifier l'évaluation que vous souhaitez désactiver.
- `--status` – Définissez cette valeur sur `INACTIVE`.

Dans l'exemple suivant, remplacez le *texte de l'espace réservé* par vos propres informations.

```
aws auditmanager update-assessment-status --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --status INACTIVE
```

Les modifications apportées à l'évaluation et à ses contrôles prennent effet au bout d'une minute environ.

Audit Manager API

Pour modifier le statut d'une évaluation en inactif à l'aide de l'API

1. Utilisez cette ListAssessmentsopération pour rechercher l'évaluation que vous souhaitez désactiver et prenez note de l'identifiant de l'évaluation.
2. Utilisez l'UpdateAssessmentStatusopération et spécifiez les paramètres suivants :
   - assessmentId : utilisez ce paramètre pour spécifier l'évaluation que vous souhaitez désactiver.
   - statut — Définissez cette valeur sur `INACTIVE`.

Les modifications apportées à l'évaluation et à ses contrôles prennent effet au bout d'une minute environ.

Pour plus d'informations sur ces opérations d'API, cliquez sur l'un des liens de la procédure précédente pour en savoir plus dans la référence des AWS Audit Manager API. Cela inclut des informations sur la façon d'utiliser ces opérations et paramètres dans l'un des SDK spécifiques au langage AWS .

Étapes suivantes

Lorsque vous êtes certain de ne plus avoir besoin de votre évaluation inactive, vous pouvez nettoyer votre environnement Audit Manager en supprimant l'évaluation. Pour obtenir des instructions, veuillez consulter Supprimer une évaluation dans AWS Audit Manager.

Supprimer une évaluation dans AWS Audit Manager

Lorsque vous n'avez plus besoin d'une évaluation, vous pouvez la supprimer de votre environnement Audit Manager. Cela vous permet de nettoyer votre espace de travail et de vous concentrer sur les évaluations correspondant à vos tâches et priorités actuelles.

> **Tip**
>
> Si votre objectif est de réduire les coûts, au lieu de supprimer une évaluation, vous pouvez modifier son statut en le configurant sur inactif. Cette action met fin à la collecte de preuves

et place votre évaluation dans un état de lecture seule par lequel vous pouvez consulter les preuves précédemment collectées. Les évaluations inactives n'entraînent aucuns frais.

Prérequis

La procédure suivante suppose que vous avez déjà créé une évaluation.

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour supprimer une évaluation dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Vous pouvez supprimer des évaluations à l'aide de la console Audit Manager, de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

Warning

Cette action entraîne la suppression définitive de votre évaluation et de toutes les preuves qu'elle a collectées. Vous ne pouvez pas récupérer ces données. Par conséquent, nous vous recommandons de procéder avec prudence et de vous assurer que vous souhaitez supprimer votre évaluation.

Audit Manager console

Pour supprimer une évaluation sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations.
3. Sélectionnez l'évaluation que vous souhaitez supprimer, puis choisissez Supprimer.

AWS CLI

Pour supprimer une évaluation dans le AWS CLI

1. Tout d'abord, identifiez l'évaluation que vous voulez supprimer. Pour ce faire, exécutez la commande list-assessments.

   ```
   aws auditmanager list-assessments
   ```

   La réponse renvoie une liste d'évaluations. Recherchez l'évaluation que vous souhaitez supprimer et prenez note de l'identifiant de l'évaluation.

2. Ensuite, utilisez la commande delete-assessment et précisez `--assessment-id` l'évaluation que vous souhaitez supprimer.

   Dans l'exemple suivant, remplacez le *texte de l'espace réservé* par vos propres informations.

   ```
   aws auditmanager delete-assessment --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

Pour supprimer une évaluation à l'aide de l'API

1. Utilisez cette ListAssessmentsopération pour rechercher l'évaluation que vous souhaitez supprimer.

   Prenez note de l'ID d'évaluation figurant dans la réponse.

2. Utilisez l'DeleteAssessmentopération et spécifiez l'ID d'évaluation de l'évaluation que vous souhaitez supprimer.

Pour plus d'informations sur ces opérations d'API, cliquez sur l'un des liens précédents dans le Guide de référence de l'API AWS Audit Manager . Il inclut des informations sur l'utilisation du fonctionnement et des paramètres dans l'un des SDK AWS spécifiques au langage.

Ressources supplémentaires

Pour plus d'informations sur la conservation des données dans Audit Manager, consultezSuppression des données d'Audit Manager.

Délégations en AWS Audit Manager

Au cours du processus d'évaluation AWS Audit Manager, vous pouvez rencontrer des situations dans lesquelles vous aurez besoin de l'aide d'experts en la matière pour examiner et valider les preuves recueillies. C'est là que le concept de délégation entre en jeu.

Points clés

Les délégations permettent aux responsables de l'audit d'attribuer des ensembles de contrôle spécifiques aux délégués, c'est-à-dire à des personnes possédant une expertise spécialisée dans les domaines concernés. En utilisant la fonction de délégation, vous pouvez vous assurer que les preuves de chaque contrôle sont soigneusement évaluées par le personnel approprié. Cela vous permet de rationaliser le processus de révision et d'améliorer la précision et la fiabilité globales de vos évaluations. Que vous ayez besoin de conseils pour interpréter les preuves techniques, clarifier les exigences de conformité ou approfondir vos connaissances dans des domaines spécifiques, les délégations vous permettent de collaborer efficacement avec des experts en la matière.

À haut niveau, le processus de délégation est le suivant :

1. Le responsable d'audit choisit une série de contrôles dans son évaluation et la délègue pour examen.
2. Le délégué examine les contrôles et leurs éléments probants, et renvoie la série de contrôles au responsable d'audit une fois terminé.
3. Le responsable d'audit est informé que la révision est terminée et consulte les remarques éventuelles laissées par le délégué concernant les contrôles examinés.

> **Note**
>
> An Compte AWS peut être propriétaire d'un audit ou délégué dans un autre domaine Régions AWS.

Ressources supplémentaires

Consultez les sections suivantes de ce chapitre pour en savoir plus sur la gestion des tâches de délégation dans AWS Audit Manager.

Comprendre les différentes tâches de délégation pour les responsables de l'audit

En tant que responsable de l'audit dans AWS Audit Manager, vous êtes chargé de gérer les évaluations et de garantir la conformité au sein de votre organisation. Bien que vous possédiez une expertise en matière de gouvernance, de risque et de conformité, il peut arriver que vous ayez des questions ou que vous ayez besoin de l'aide d'experts en la matière pour examiner et interpréter des preuves ou des contrôles techniques spécifiques. C'est là que la fonctionnalité de délégation d'Audit Manager devient utile.

Points clés

La création d'une délégation vous permet d'attribuer des ensembles de contrôle dans le cadre d'une évaluation à d'autres utilisateurs d'Audit Manager (appelés délégués) qui possèdent des connaissances spécialisées ou une expertise technique dans les domaines concernés. Ces délégués peuvent ensuite examiner les ensembles de contrôles assignés, analyser les preuves collectées, fournir des commentaires ou des preuves supplémentaires si nécessaire, et mettre à jour le statut des contrôles individuels.

Le processus de délégation rationalise l'examen et la validation des contrôles en tirant parti de l'expertise collective au sein de votre organisation. Cela garantit que chaque contrôle est soigneusement évalué par le personnel le plus qualifié, améliorant ainsi la précision et la fiabilité de vos évaluations.

Ressources supplémentaires

Les sections suivantes vous guident à travers les différentes tâches associées à la gestion des délégations en tant que responsable de l'audit. Cela inclut la manière de déléguer des ensembles de contrôle, de suivre le statut des délégations et de gérer les délégations terminées. En utilisant efficacement les délégations, vous pouvez collaborer avec des experts en la matière, tirer parti de leurs connaissances spécialisées et maintenir un processus d'audit complet et bien informé au sein d'Audit Manager.

- Délégation d'un ensemble de contrôles pour révision dans AWS Audit Manager
- Trouver et examiner les délégations que vous avez envoyées AWS Audit Manager
- Suppression de vos délégations terminées dans AWS Audit Manager

Délégation d'un ensemble de contrôles pour révision dans AWS Audit Manager

Lorsque vous avez besoin de l'aide d'un expert en la matière, vous pouvez choisir Compte AWS celui qui vous convient, puis lui déléguer un ensemble de contrôles pour qu'il le révise.

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour créer une délégation dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont Permettre aux utilisateurs un accès administrateur complet à AWS Audit Manager etAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Vous pouvez utiliser l'une des procédures suivantes pour déléguer une série de contrôles.

Délégation d'une série de contrôles sur une page d'évaluation

Pour déléguer une série de contrôles sur la page d'évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations.

3. Sélectionnez le nom de l'évaluation contenant la série de contrôles que vous souhaitez déléguer.
4. Sur la page d'évaluation, choisissez l'onglet Contrôles. Le résumé de l'état des contrôles et la liste des contrôles compris dans l'évaluation s'affichent.
5. Sélectionnez une série de contrôles, puis choisissez Déléguer cette série de contrôles.
6. Sous Sélection du délégué, une liste d'utilisateurs et de rôles s'affiche. Choisissez un utilisateur ou un rôle, ou recherchez-le dans la barre de recherche.
7. Sous Détails de la délégation, vérifiez le nom de la série de contrôles et le nom de l'évaluation.
8. (Facultatif) Sous Commentaires, ajoutez un commentaire contenant des instructions pour aider le délégué à accomplir sa tâche d'examen. N'incluez aucune information sensible dans votre commentaire.
9. Choisissez Déléguer cette série de contrôle.
10. Une bannière verte confirme que la série de contrôles a été déléguée avec succès. Choisissez Afficher la délégation pour voir la demande de délégation. Vous pouvez également consulter vos délégations à tout moment en choisissant Délégations dans le volet de navigation de gauche de la AWS Audit Manager console.

Délégation d'une série de contrôles sur la page des délégations

Pour déléguer une série de contrôles sur la page des délégations

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, sélectionnez Délégations.
3. Sur la page des délégations, choisissez Créer une délégation.
4. Sous Choisir une évaluation et une série de contrôles, spécifiez l'évaluation et la série 'de contrôles que vous souhaitez déléguer.
5. Sous Sélection du délégué, une liste d'utilisateurs et de rôles s'affiche. Choisissez un utilisateur ou un rôle, ou recherchez-le dans la barre de recherche.
6. (Facultatif) Sous Commentaires, ajoutez un commentaire contenant des instructions pour aider le délégué à accomplir sa tâche d'examen. N'incluez aucune information sensible dans votre commentaire.
7. Cliquez sur Créer une délégation.
8. Une bannière verte confirme que la série de contrôles a été déléguée avec succès. Choisissez Afficher la délégation pour voir la demande de délégation. Vous pouvez également consulter vos

délégations à tout moment en choisissant Délégations dans le volet de navigation de gauche de la AWS Audit Manager console.

Une fois que vous avez délégué un ensemble de contrôles à des fins de révision, le délégué reçoit une notification et peut alors commencer à revoir l'ensemble de contrôles. Ce processus effectué par les délégués est décrit dans Comprendre les différentes tâches de délégation pour les délégués.

Étapes suivantes

Pour revoir votre délégation à une date ultérieure, voirTrouver et examiner les délégations que vous avez envoyées AWS Audit Manager.

Trouver et examiner les délégations que vous avez envoyées AWS Audit Manager

Vous pouvez accéder à la liste de vos délégations à tout moment en choisissant Délégations dans le volet de navigation de gauche d'Audit Manager. La page des délégations contient la liste de vos délégations actives et terminées.

Lorsqu'une délégation est terminée, vous recevez une notification dans Audit Manager. Vous pouvez également recevoir des commentaires accompagnés de remarques de la part du délégué. La procédure suivante explique comment vérifier vos délégations dans Audit Manager une fois qu'elles sont terminées, et comment afficher les commentaires que le délégué pourrait vous avoir laissés.

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour consulter une délégation. AWS Audit Manager Les deux politiques suggérées pour accorder ces autorisations sont Permettre aux utilisateurs un accès administrateur complet à AWS Audit Manager etAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Suivez ces étapes pour rechercher et consulter les délégations que vous avez créées précédemment.

Pour consulter une délégation terminée et vérifier les commentaires

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, sélectionnez Délégations.
3. Consultez la page Délégations, qui inclut un tableau contenant les informations suivantes :

Name (Nom)	Description
Délégué à	Celui Compte AWS auquel vous avez délégué le contrôle est défini.
Date	Date à laquelle vous avez délégué le jeu de contrôle.
Statut	Le statut actuel de la délégation.
Évaluation	Le nom de l'évaluation avec un lien vers la page détaillée de l'évaluation.
Kit de commande	Nom de l'ensemble de contrôles qui a été délégué pour révision.

4. Recherchez l'évaluation et la série de contrôles que le délégué a examinée et vous a soumise, puis sélectionnez le nom de l'évaluation pour l'ouvrir.
5. Sous l'onglet Contrôles de la page détaillée de l'évaluation, faites défiler la page vers le bas jusqu'au tableau Séries de contrôles.
6. Sous Contrôles regroupés par ensemble de contrôles, recherchez le nom du jeu de contrôles que vous avez délégué.
7. Développez le nom du jeu de contrôles pour afficher ses contrôles, puis choisissez le nom d'un contrôle pour ouvrir la page détaillée du contrôle.
8. Cliquez sur l'onglet Commentaires pour afficher les remarques ajoutées par le délégué pour ce contrôle en particulier.
9. Lorsque vous êtes convaincu que la révision d'un ensemble de commandes est terminée, sélectionnez le jeu de commandes, puis choisissez Révision complète du jeu de commandes.

> **Important**
>
> Audit Manager recueille des éléments probants en permanence. Par conséquent, de nouveaux éléments probants peuvent être recueillis après que le délégué ait terminé l'examen d'un contrôle.
> Si vous souhaitez uniquement utiliser les éléments probants examinés dans vos rapports d'évaluation, vous pouvez vous référer à l'horodatage de la série de contrôles pour savoir à quel moment les éléments probants ont été examinés. Cet horodatage se trouve sur la page détaillée Onglet Journal des modifications du contrôle. Il vous permettra ensuite d'identifier les éléments probants à ajouter à vos rapports d'évaluation.

Étapes suivantes

Pour supprimer une délégation une fois qu'elle est terminée et que vous n'en avez plus besoin, consultezSuppression de vos délégations terminées dans AWS Audit Manager.

Suppression de vos délégations terminées dans AWS Audit Manager

Il peut arriver que vous créiez une délégation, mais que vous n'ayez plus besoin d'aide par la suite pour examiner cette série de contrôles. Dans ce cas, vous pouvez supprimer une délégation active dans Audit Manager. Vous pouvez également supprimer les délégations terminées que vous ne souhaitez plus voir sur la page des délégations.

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour supprimer une délégation. AWS Audit Manager Les deux politiques suggérées pour accorder ces autorisations sont Permettre aux utilisateurs un accès administrateur complet à AWS Audit Manager etAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Pour supprimer une délégation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, sélectionnez Délégations.

3. Sur la page Délégations, sélectionnez la délégation que vous souhaitez annuler, puis choisissez Supprimer la délégation.
4. Dans la fenêtre contextuelle qui apparaît, choisissez Supprimer pour confirmer votre choix.

Comprendre les différentes tâches de délégation pour les délégués

En tant que délégué AWS Audit Manager, vous jouez un rôle important en soutenant les responsables de l'audit au cours du processus d'évaluation. Bien que les responsables de l'audit soient chargés de gérer les évaluations et de garantir la conformité globale, ils peuvent parfois avoir besoin de l'aide d'experts en la matière pour examiner et interpréter des preuves techniques spécifiques qui ne relèvent pas de leur domaine d'expertise. Dans de tels scénarios, vos connaissances et vos compétences deviennent inestimables.

Points clés

La fonction de délégation permet aux responsables de l'audit de vous attribuer des ensembles de contrôles spécifiques pour examen, en tirant parti de votre expertise commerciale ou technique spécialisée. Cette approche collaborative améliore non seulement la précision et la fiabilité des évaluations, mais rationalise également le processus d'examen, permettant aux responsables des audits de se concentrer sur leurs principales responsabilités, tandis que vous concentrez vos efforts sur les domaines dans lesquels votre expertise est la plus précieuse.

En tant que délégué, vous pouvez recevoir des demandes de la part des responsables de l'audit pour examiner les éléments probants associés aux ensembles de contrôle assignés. Vous pouvez aider les responsables d'audit en examinant les séries de contrôles et les éléments probants associés, en ajoutant des commentaires, en téléchargeant des éléments probants supplémentaires et en mettant à jour le statut de chaque contrôle que vous examinez.

> **Note**
>
> Les responsables d'audit délèguent des séries de contrôles spécifiques, et non des évaluations complètes, pour examen. Par conséquent, les délégués ont un accès limité aux évaluations. Les délégués peuvent examiner les éléments probants, ajouter des commentaires, télécharger des éléments probants manuels et mettre à jour l'état des contrôles pour chacun des contrôles de la série. Pour plus d'informations sur les rôles et les

autorisations dans Audit Manager, consultez Politiques recommandées pour les personas utilisateurs dans AWS Audit Manager.

Ressources supplémentaires

Dans les sections suivantes, vous pouvez en savoir plus sur les tâches associées à la gestion des délégations en tant que délégué. Cela inclut la manière de consulter les demandes de délégation entrantes, de passer en revue les ensembles de contrôles assignés, de fournir des commentaires et des preuves supplémentaires, et de renvoyer vos contrôles révisés au responsable de l'audit.

- Affichage de vos notifications pour les demandes de délégation entrantes
- Examen de la série de contrôles déléguée et des éléments probants connexes
- Ajouter des commentaires à propos d'un contrôle lors de la révision d'un ensemble de contrôles
- Marquage d'un contrôle tel qu'il est examiné dans AWS Audit Manager
- Soumission d'un ensemble de contrôles vérifié au responsable de l'audit

Affichage de vos notifications pour les demandes de délégation entrantes

Lorsqu'un responsable d'audit vous demande de l'aide pour examiner une série de contrôles, vous recevez une notification vous informant qu'une série de contrôles vous a été déléguée.

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour consulter les notifications. AWS Audit Manager Les deux politiques suggérées pour accorder ces autorisations sont Permettre aux utilisateurs un accès administrateur complet à AWS Audit Manager etAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Pour afficher vos notifications

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Notifications.

3. Sur la page Notifications, vous pouvez consulter la liste des séries de contrôles qui vous ont été déléguées pour examen. Le tableau comprend les informations suivantes :

Name (Nom)	Description
Date	Date à laquelle l'ensemble de contrôle a été délégué.
Évaluation	Nom de l'évaluation associée à l'ensemble de contrôles.
Kit de commande	Nom du jeu de commandes.
Source	L'utilisateur ou le rôle qui vous a délégué le jeu de contrôle.
Description	Instructions fournies par le responsable de l'audit.

> **Tip**
>
> Vous pouvez également vous abonner à une rubrique SNS pour recevoir des alertes par e-mail lorsqu'une série de contrôles vous est déléguée pour examen. Pour plus d'informations, consultez Notifications dans AWS Audit Manager.

Étapes suivantes

Lorsque vous serez prêt à passer en revue les contrôles qui vous ont été délégués, consultezExamen de la série de contrôles déléguée et des éléments probants connexes.

Examen de la série de contrôles déléguée et des éléments probants connexes

Vous pouvez aider les responsables d'audit en vérifiant les séries de contrôles qu'ils vous ont délégués.

En examinant les contrôles et leurs éléments probants, vous pouvez déterminer si une action supplémentaire est nécessaire. Ces actions supplémentaires peuvent être le téléchargement manuel d'éléments probants supplémentaires pour démontrer la conformité, ou l'ajout d'un commentaire détaillant les étapes de correction effectuées.

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour afficher un contrôle défini dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont Permettre aux utilisateurs un accès administrateur complet à AWS Audit Manager etAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Pour vérifier un ensemble de contrôles

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation, choisissez Notifications.
3. Sur la page Notifications, vous pouvez voir la liste des ensembles de contrôles qui vous ont été délégués. Identifiez la série de contrôles que vous souhaitez examiner et choisissez le nom de l'évaluation associée pour ouvrir sa page détaillée.
4. Sous l'onglet Contrôles de la page détaillée de l'évaluation, faites défiler la page vers le bas jusqu'au tableau Séries de contrôles.
5. Dans la colonne Contrôles regroupés par séries de contrôles, cliquez sur le nom d'une série de contrôles pour en afficher le détail.
6. Choisissez le nom d'un contrôle pour ouvrir la page détaillée du contrôle.
7. (Facultatif) Choisissez Mettre à jour le statut du contrôle pour modifier le statut du contrôle. Pendant que votre vérification est en cours, vous pouvez marquer le statut comme En cours de vérification.
8. Consultez les informations relatives au contrôle dans les dossiers Preuves, Détails, Sources de données, Commentaires et Changelog.

    - Pour en savoir plus sur chacun de ces onglets et sur la façon de comprendre les données qu'ils contiennent, consultezRévision d'un contrôle d'évaluation dans AWS Audit Manager.

Pour vérifier les éléments probants d'un contrôle

1. Sur la page détaillée du contrôle, choisissez l'onglet Dossiers d'éléments probants.

2. Accédez au tableau des dossiers de preuves pour voir la liste des dossiers contenant des preuves relatives à ce contrôle. Ces dossiers sont organisés et nommés en fonction de la date à laquelle les éléments probants ont été recueillis.
3. Sélectionnez le nom d'un dossier d'éléments probants pour l'ouvrir. Puis, vous pouvez consulter un résumé de tous les éléments probants recueillis à cette date.

   - Ce résumé inclut le nombre total de problèmes de contrôle de conformité signalés directement AWS Security Hub ou par les deux. AWS Config
   - Pour en savoir plus sur ces informations, consultezRévision d'un dossier de preuves dans AWS Audit Manager.
4. À partir de la page récapitulative du dossier d'éléments probants, accédez au tableau éléments probants. Dans la colonne Heure, choisissez un élément de preuve à ouvrir.
5. Passez en revue les détails des preuves.

   - Pour en savoir plus sur ces informations, consultezExamen des preuves dans AWS Audit Manager.

Étapes suivantes

Dans certains cas, vous devrez peut-être fournir des preuves supplémentaires pour démontrer la conformité. Dans ces cas, vous pouvez télécharger manuellement les éléments probants. Pour obtenir des instructions, veuillez consulter Ajouter des preuves manuelles dans AWS Audit Manager.

Si vous souhaitez laisser des commentaires sur un ou plusieurs des contrôles qui vous ont été délégués, consultezAjouter des commentaires à propos d'un contrôle lors de la révision d'un ensemble de contrôles.

Ajouter des commentaires à propos d'un contrôle lors de la révision d'un ensemble de contrôles

Vous pouvez ajouter des commentaires pour tous les contrôles que vous vérifiez. Ces commentaires sont visibles par le responsable de l'audit.

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour ajouter des commentaires à un contrôle d'évaluation dans AWS Audit Manager. Les deux politiques suggérées

pour accorder ces autorisations sont Permettre aux utilisateurs un accès administrateur complet à AWS Audit Manager etAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Pour ajouter un commentaire à un contrôle

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Notifications.
3. Sur la page Notifications, vérifiez la liste des séries de contrôles qui vous ont été déléguées.
4. Recherchez le jeu de contrôles contenant le contrôle pour lequel vous souhaitez laisser un commentaire, puis choisissez le nom de l'évaluation associée pour ouvrir l'évaluation.
5. Choisissez l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'à Ensembles de contrôles, puis sélectionnez le nom d'un contrôle pour l'ouvrir.
6. Sélectionnez l'onglet Commentaires.
7. Sous Envoyer des commentaires, saisissez votre commentaire dans la zone de texte.
8. Choisissez Soumettre un commentaire pour ajouter votre commentaire. Votre commentaire apparaît ensuite dans la section Commentaires précédents de la page, avec tout autre commentaire concernant ce contrôle.

Étapes suivantes

Lorsque vous avez terminé de vérifier le contrôle, suivez les étapes décrites dansMarquage d'un contrôle tel qu'il est examiné dans AWS Audit Manager.

Marquage d'un contrôle tel qu'il est examiné dans AWS Audit Manager

Vous pouvez indiquer la progression de votre révision en mettant à jour le statut des contrôles individuels d'une série de contrôles.

La modification du statut d'un contrôle est facultative. Cependant, nous vous recommandons de modifier le statut de chaque contrôle sur Vérifié au fur et à mesure de votre vérification de ce contrôle. Quel que soit le statut de chaque contrôle individuel, vous pouvez toujours renvoyer les contrôles au responsable d'audit.

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour mettre à jour le statut d'un contrôle d'évaluation dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont Permettre aux utilisateurs un accès administrateur complet à AWS Audit Manager etAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Pour marquer un contrôle comme vérifié

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Notifications.
3. Sur la page Notifications, vérifiez la liste des séries de contrôles qui vous ont été déléguées.
4. Recherchez l'ensemble de contrôles que vous souhaitez marquer comme révisé, puis choisissez le nom de l'évaluation associée pour ouvrir l'évaluation.
5. Sous l'onglet Contrôles de la page détaillée de l'évaluation, faites défiler la page vers le bas jusqu'au tableau Séries de contrôles.
6. Dans la colonne Contrôles regroupés par séries de contrôles, cliquez sur le nom d'une série de contrôles pour en afficher le détail.
7. Choisissez le nom d'un contrôle pour ouvrir la page détaillée du contrôle.
8. Choisissez Mettre à jour le statut du contrôle et remplacez le statut par Vérifié.
9. Dans la fenêtre contextuelle qui apparaît, choisissez Mettre à jour le statut du contrôle pour confirmer que vous avez terminé de vérifier le contrôle.

Étapes suivantes

Pour terminer le processus de délégation, voirSoumission d'un ensemble de contrôles vérifié au responsable de l'audit.

Soumission d'un ensemble de contrôles vérifié au responsable de l'audit

Après avoir examiné l'ensemble de contrôles, ajouté des commentaires ou des éléments de preuve supplémentaires et mis à jour le statut de chaque contrôle, vous franchissez une étape importante : renvoyer le jeu de contrôles révisé au responsable de l'audit. La soumission de l'ensemble de

contrôles révisé marque l'achèvement de vos tâches déléguées et permet au responsable de l'audit d'intégrer vos informations et recommandations dans l'évaluation globale.

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour soumettre le set de contrôle révisé au propriétaire de l'audit dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont Permettre aux utilisateurs un accès administrateur complet à AWS Audit Manager etAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Procédez comme suit pour soumettre le jeu de contrôles au propriétaire de l'audit.

Pour renvoyer une série de contrôles vérifiée au responsable de l'audit

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Notifications.
3. Consultez la liste des séries de contrôles qui vous ont été déléguées. Recherchez la série de contrôles que vous souhaitez renvoyer au responsable de l'audit, puis cliquez sur le nom de l'évaluation associée.
4. Faites défiler la page jusqu'au tableau Séries de contrôles, sélectionnez la série de contrôles que vous souhaitez envoyer au responsable d'audit, puis cliquez sur Envoyer pour examen.
5. Dans la fenêtre contextuelle qui apparaît, vous pouvez ajouter des commentaires avant de choisir Envoyer pour examen.

Rapports d'évaluation

Un rapport d'évaluation résume les éléments probants sélectionnés qui ont été recueillis pour une évaluation. Il contient également des liens vers des fichiers PDF contenant des détails sur chaque élément probant. Le contenu, l'organisation et la convention de dénomination spécifiques d'un rapport d'évaluation dépendent des paramètres que vous choisissez lorsque vous générez le rapport.

Les rapports d'évaluation vous aident à sélectionner et à compiler les éléments probants pertinents pour votre audit. Cependant, ils n'évaluent pas la conformité des éléments probants eux-mêmes. Au lieu de cela, Audit Manager fournit simplement les détails des éléments probants sélectionnés sous forme de sortie que vous pouvez partager avec votre auditeur.

Table des matières

Comprendre la structure des dossiers des rapports d'évaluation

Lorsque vous téléchargez un rapport d'évaluation, Audit Manager crée un dossier zip. Il contient votre rapport d'évaluation et les fichiers d'éléments probants connexes dans des sous-dossiers imbriqués.

Le dossier zip est structuré comme suit :

- Dossier d'évaluation (exemple : `myAssessmentName-a1b2c3d4`) - Le dossier racine.
  - Dossier du rapport d'évaluation (exemple :`reportName-a1b2c3d4e5f6g7`) — Sous-dossier dans lequel se trouvent les AssessmentReportSummary fichiers .pdf, digest.txt et README.txt.
    - Dossier d'éléments probants par contrôle (exemple : `controlName-a1b2c3d4e5f6g`) - Sous-dossier qui regroupe les fichiers d'éléments probants en fonction du contrôle correspondant.
      - Dossier d'éléments probants par source de données (exemple : `CloudTrail`,`Security Hub`) - Sous-dossier qui regroupe les fichiers d'éléments probants par type de source de données.
        - Dossier d'éléments probants par date (exemple : `2022-07-01`) - Sous-dossier qui regroupe les fichiers d'éléments probants en fonction de la date de collecte des éléments probants.
          - Fichiers d'éléments probants - Fichiers qui contiennent des détails sur des éléments probants individuels.

Naviguer dans un rapport d'évaluation

Commencez par ouvrir le dossier zip et naviguez d'un niveau vers le bas jusqu'au dossier du rapport d'évaluation. Vous trouverez ici le rapport d'évaluation au format PDF et le fichier README.txt.

Vous pouvez consulter le fichier README.txt pour comprendre la structure et le contenu du dossier zip. Il fournit également des informations de référence sur les conventions de dénomination de chaque fichier. Ces informations peuvent vous aider à accéder directement à un sous-dossier ou à un fichier d'éléments probants si vous recherchez un élément spécifique.

Sinon, pour parcourir les éléments probants et trouver les informations dont vous avez besoin, ouvrez le rapport d'évaluation au format PDF. Vous obtenez un aperçu général du rapport et un résumé de l'évaluation qui a servi de base à la création du rapport.

Ensuite, utilisez la table des matières (TOC) pour explorer le rapport. Vous pouvez choisir n'importe quel contrôle hypertexte dans la table des matières pour accéder directement à un résumé de ce contrôle.

Lorsque vous êtes prêt à vérifier les détails des éléments probants pour un contrôle, vous pouvez le faire en choisissant le nom des éléments probants en lien hypertexte. Pour les éléments probants

automatisés, le lien hypertexte ouvre un nouveau fichier PDF contenant des détails sur ces éléments probants. Pour les éléments probants manuels, le lien hypertexte vous dirige vers le compartiment S3 qui contient les éléments probants.

> **Tip**
>
> La piste de navigation en haut de chaque page indique votre position actuelle dans le rapport d'évaluation lorsque vous parcourez les contrôles et les éléments probants. Sélectionnez le lien hypertexte de la table des matières pour revenir à cette dernière à tout moment.

Révision des sections d'un rapport d'évaluation

Utilisez les informations suivantes pour en savoir plus sur chaque section d'un rapport d'évaluation.

> **Note**
>
> Lorsqu'un trait d'union (-) apparaît à côté de l'un des attributs dans les sections suivantes, cela indique que la valeur de cet attribut est nulle ou qu'il n'existe aucune valeur.

- Page de couverture
- Page d'aperçu
- Page de table des matières
- Page de contrôle
- Page récapitulative des éléments probants
- Page détaillée des éléments probants

Page de couverture

La page de couverture inclut le nom du rapport d'évaluation. Elle affiche également la date et l'heure de génération du rapport, ainsi que l'ID de compte de l'utilisateur qui a généré le rapport.

La page de couverture est formatée comme suit. Audit Manager remplace les *`espaces réservés`* par les informations pertinentes pour votre rapport.

```
Assessment report name
Report generated on MM/DD/YYYY at HH:MM:SS AM/PM UCT by AccountID
```

Page d'aperçu

La page d'aperçu comporte deux parties : un résumé du rapport lui-même et un résumé de l'évaluation faisant l'objet du rapport.

Rapports récapitulatifs

Cette section résume le rapport d'évaluation.

Name (Nom)	Description
Nom du rapport	Nom du rapport.
Description	Description saisie par le responsable de l'audit lorsqu'il génère le rapport.
Date de génération	Date à laquelle le rapport a été généré. L'heure est représentée au format UTC (temps universel coordonné).
Nombre total de commandes incluses	Le nombre de contrôles inclus dans le rapport et pour lesquels des preuves ont été recueillies. Il s'agit d'un sous-ensemble du nombre total de contrôles inclus dans l'évaluation.
Comptes AWS inclus	Le nombre d'entre Comptes AWS eux sont inclus dans le rapport et ont permis de recueillir des preuves. Il s'agit d'un sous-ense mble du nombre total de personnes incluses Comptes AWS dans l'évaluation.
Sélection du rapport d'évaluation	Le nombre d'éléments de preuve sélectionnés pour être inclus dans le rapport. Cela inclut le nombre total de problèmes de vérification de conformité détectés dans le rapport.

Résumé de l'évaluation

Cette section résume l'évaluation à laquelle se rapporte le rapport.

Name (Nom)	Description
Nom de l'évaluation	Nom de l'évaluation à partir de laquelle le rapport a été généré.
Statut	État de l'évaluation au moment où le rapport a été généré.
Région d'évaluation	Le dans Région AWS lequel l'évaluation a été créée.
Comptes AWS dans le champ d'application	La liste de ces Comptes AWS éléments s'inscrit dans le cadre de l'évaluation.
Nom du framework	Nom du cadre à partir duquel l'évaluation a été créée.
Propriétaires de l'audit	L'utilisateur ou le rôle des responsables de l'audit de l'évaluation.
Dernière mise à jour	Date à laquelle l'évaluation a été mise à jour pour la dernière fois. L’heure indique l’heure UTC.

Page de table des matières

La table des matières affiche le contenu complet du rapport d’évaluation. Le contenu est regroupé et organisé en fonction des ensembles de contrôle inclus dans l’évaluation. Les commandes sont répertoriées sous leur ensemble de commandes respectif.

Choisissez n’importe quel élément dans la table des matières pour accéder directement à cette section du rapport. Vous pouvez choisir un ensemble de commandes ou accéder directement à une commande.

Page de contrôle

La page de contrôle comporte deux parties : un résumé du contrôle lui-même et un résumé des éléments probants collectés pour le contrôle.

Résumé des contrôles

Cette section comprend les informations suivantes.

Name (Nom)	Description
Nom du contrôle	Le nom du contrôle.
Description	Description du contrôle.
Kit de commande	Nom du jeu de contrôles auquel appartient le contrôle.
Informations sur les tests	Les procédures de test recommandées pour ce contrôle.
Plan d'action	Les actions recommandées à effectuer si le contrôle n'est pas rempli.
Sélection du rapport d'évaluation	Le nombre d'éléments de preuve liés à ce contrôle qui ont été inclus dans le rapport d'évaluation. Cela inclut le nombre de problèmes de contrôle de conformité détectés pour les éléments probants de ce contrôle.

Éléments probants recueillis

Cette section présente les éléments probants recueillis pour le contrôle. Les éléments probants sont regroupés par dossiers, qui sont organisés et nommés en fonction de la date de collecte des éléments probants. À côté du nom de chaque dossier d'éléments probants figure le nombre total de problèmes de contrôle de conformité pour ce dossier.

Sous le nom de chaque dossier d'éléments probants se trouve une liste de noms d'éléments probants liés par des hyperliens.

- Les noms d'éléments probants automatisés commencent par un horodatage de collecte d'éléments probants, suivi du code de service, du nom de l'événement (jusqu'à 20 caractères), de l'identifiant du compte et d'un identifiant unique à 12 caractères.

  Par exemple : `21-30-24_IAM_CreateUser_111122223333_a1b2c3d4e5f6`

  Pour les éléments probants automatisés, le nom du lien hypertexte ouvre un nouveau fichier PDF contenant un résumé et des informations supplémentaires.
- Les noms d'éléments probants manuels commencent par un horodatage de téléchargement des éléments probants, suivi de l'étiquette `manual`, de l'identifiant du compte et d'un identifiant unique

à 12 caractères. Ils incluent également les 10 premiers caractères du nom du fichier, ainsi que l'extension du fichier (10 caractères maximum).

Par exemple : `00-00-00_manual_111122223333_a1b2c3d4e5f6_myimage.png`

Pour les éléments probants manuels, le nom du lien hypertexte vous dirige vers le compartiment S3 qui contient les éléments probants.

À côté de chaque nom d'élément probant figure le résultat du contrôle de conformité de cet élément.

- Pour les preuves automatisées collectées auprès de AWS Security Hub ou AWS Config, un résultat conforme, non conforme ou non concluant est signalé.
- Pour les preuves automatisées collectées à partir d' AWS CloudTrail appels d'API, et pour toutes les preuves manuelles, un résultat non concluant est affiché.

Page récapitulative des éléments probants

La page de résumé des preuves contient les informations suivantes.

Name (Nom)	Description
ID	L'identifiant unique des preuves.
Date de collecte	Date à laquelle les preuves ont été créées ou téléchargées.
Description	Description des preuves, y compris l'identifiant du compte et le type de source de données.
Nom de l'évaluation	Nom de l'évaluation à partir de laquelle le rapport a été généré.
Nom du framework	Nom du cadre à partir duquel l'évaluation a été créée.
Nom du contrôle	Le nom du contrôle étayé par les preuves.
Nom du jeu de commandes	Nom du jeu de contrôles auquel appartient le contrôle associé.
Description du contrôle	Description du contrôle étayé par les preuves.
Informations sur les tests	Les procédures de test recommandées pour le contrôle.

Name (Nom)	Description
Plan d'action	Les actions recommandées à effectuer si le contrôle n'est pas rempli.
Région AWS	Le nom de la région associée aux preuves.
ID IAM	L'ARN de l'utilisateur ou du rôle associé aux preuves.
Compte AWS	L' Compte AWS identifiant associé aux preuves.
Service AWS	Le nom de Service AWS la personne associée aux preuves.
Nom de l’événement	Le nom de l'événement de preuve.
Heure de l’événement	Heure à laquelle l'événement de preuve s'est produit.
Source de données	L'endroit d'où les preuves ont été collectées ou téléchargées. Le type de source de données peut être Security Hub CloudTrail, appels d' AWS API ou manuel. AWS Config
Preuve par type	La catégorie de preuves • Les preuves du contrôle de conformité sont collectées auprès de AWS Config notre Security Hub. • Les preuves de l'activité des utilisateurs sont collectées à partir CloudTrail des journaux. • Les preuves des données de configuration sont collectées à partir d'instantanés d'autres Services AWS. • Les éléments probants manuels sont des éléments probants que vous chargez manuellement.

Name (Nom)	Description
État du contrôle de conformité	État d'évaluation des preuves relevant de la catégorie des contrôles de conformité. • Pour les preuves automatisées collectées auprès de AWS Security Hub ou AWS Config, un résultat conforme, non conforme ou non concluant est signalé. • Pour les preuves automatisées collectées à partir d' AWS CloudTrail appels d'API, et pour toutes les preuves manuelles, un résultat non concluant est affiché.

Page détaillée des éléments probants

La page détaillée des éléments probants indique le nom de l'élément probant et un tableau détaillé des éléments probants. Ce tableau fournit une analyse détaillée de chaque élément probant afin que vous puissiez comprendre les données et valider leur exactitude. En fonction de la source de données des éléments probants, le contenu de la page détaillée des éléments probants varie.

> **Tip**
>
> La piste de navigation en haut de chaque page indique votre position actuelle dans le rapport d'évaluation lorsque vous parcourez les éléments probants détaillés. Sélectionnez Résumé des éléments probants pour revenir au résumé des éléments probants à tout moment.

Validation d'un rapport d'évaluation

Lorsque vous générez un rapport d'évaluation, Audit Manager produit une somme de contrôle du fichier de rapport appelée `digest.txt`. Vous pouvez utiliser ce fichier pour valider l'intégrité du rapport et vous assurer qu'aucun élément probant n'a été modifié après la création du rapport. Il contient un objet JSON avec des signatures et des hachages qui sont invalidés si une partie de l'archive de rapports est modifiée.

Pour valider l'intégrité d'un rapport d'évaluation, utilisez l'ValidateAssessmentReportIntegrityAPI fournie par Audit Manager.

Ressources supplémentaires

Pour trouver des réponses aux questions et problèmes courants, consultez Résolution des problèmes liés aux rapports d'évaluation la section Dépannage de ce guide.

Outil de recherche d'éléments probants

L'outil de recherche d'éléments probants est un puissant moyen de rechercher des éléments probants dans Audit Manager. Au lieu de parcourir des dossiers d'éléments probants profondément enfouis et difficiles d'accès pour trouver ce que vous recherchez, l'outil de recherche d'éléments probants est beaucoup plus rapide. Si vous utilisez la recherche d'éléments probants en tant qu'administrateur délégué, vous pouvez inclure tous les comptes membres de votre organisation dans votre recherche.

Vous pouvez affiner votre requête de recherche à l'aide de filtres et de regroupements. Par exemple, si vous souhaitez obtenir une vue d'ensemble de l'état de votre système, effectuez une recherche approfondie et filtrez par évaluation, plage de dates et conformité des ressources. Si votre objectif est de remédier à une ressource spécifique, vous pouvez effectuer une recherche précise afin de cibler les éléments probants d'un contrôle ou d'un identifiant de ressource spécifique. Après avoir défini vos filtres, vous pouvez regrouper puis prévisualiser les résultats de recherche correspondants, avant de créer un rapport d'évaluation.

Pour utiliser l'outil de recherche d'éléments probants, vous devez activer cette fonctionnalité dans les paramètres de l'Audit Manager.

Points clés

Comprendre comment fonctionne Evidence Finder avec CloudTrail Lake

L'outil de recherche d'éléments probants utilise les capacités de requête et de stockage d'AWS CloudTrail Lake. Avant de commencer à utiliser Evidence Finder, il est utile d'en savoir un peu plus sur CloudTrail le fonctionnement de Lake.

CloudTrail Lake regroupe les données dans un seul magasin de données d'événements consultable qui prend en charge de puissantes requêtes SQL. Vous pouvez ainsi effectuer des recherches dans toute votre organisation et sur des plages horaires personnalisées. L'outil de recherche d'éléments probants vous permet d'utiliser cette fonctionnalité de recherche directement sur la console Audit Manager.

Lors de la demande d'activation de l'outil de recherche d'éléments probants, Audit Manager crée un entrepôt de données d'événements en votre nom. Une fois l'outil de recherche d'éléments probants

activé, tous vos futurs éléments probants Audit Manager sont ingérés dans l'entrepôt de données d'événements, où ils sont disponibles pour recherche. Une fois l'outil de recherche d'éléments probants activé, l'entrepôt de données d'événements nouvellement créé se remplit automatiquement des données d'éléments probants de ces deux dernières années. Si vous activez l'outil de recherche d'éléments probants en tant qu'administrateur délégué, les données de tous les comptes membres de votre organisation seront renseignées.

Toutes vos données d'éléments probants, qu'elles soient remplies rétroactivement ou nouvelles, sont conservées dans l'entrepôt de données d'événements pendant 2 ans. Vous pouvez modifier la période de conservation par défaut à tout moment. Pour des instructions plus détaillées, consultez la section Update an event data store du guide de l'utilisateur AWS CloudTrail . Vous pouvez conserver les données d'événement dans un entrepôt de données d'événement pendant sept ans maximum (soit 2 555 jours).

> **Note**
>
> Lorsque de nouvelles données probantes sont ajoutées au magasin de données sur les événements, des frais de CloudTrail Lake sont facturés pour le stockage et l'ingestion des données.
> Pour les requêtes CloudTrail Lake, vous payez au fur et à mesure. Cela signifie que pour chaque requête de recherche effectuée dans l'outil de recherche d'éléments probants, les données analysées vous sont facturées.
> Pour plus d'informations sur la tarification CloudTrail du lac, consultez la section AWS CloudTrail Tarification.

Étapes suivantes

Pour commencer, activez l'outil de recherche de preuves dans les paramètres de l'Audit Manager. Pour obtenir des instructions, veuillez consulter Activation de l'outil de recherche d'éléments probants.

Ressources supplémentaires

- Recherche de preuves dans Evidence Finder
- Affichage des résultats dans l'outil de recherche d'éléments probants
- Options de filtrage et de regroupement pour l'outil de recherche de preuves

- Exemples de cas d'utilisation de l'outil de recherche de preuves
- Résolution des problèmes liés à l'outil de recherche d'éléments probants

Recherche de preuves dans Evidence Finder

Vous pouvez utiliser l'outil de recherche de preuves pour effectuer des recherches ciblées et trouver rapidement des preuves pertinentes à examiner.

Sur cette page, vous apprendrez à filtrer vos recherches en fonction de critères tels que l'évaluation, la plage de dates, le statut de conformité des ressources et des attributs supplémentaires. L'application de ces filtres réduit votre champ de recherche aux seules preuves dont vous avez besoin. Vous pouvez également regrouper vos résultats en fonction de certains champs afin de mieux analyser les modèles.

Prérequis

Assurez-vous d'avoir suivi les étapes pour activer l'outil de recherche de preuves dans les paramètres de l'Audit Manager. Pour obtenir des instructions, veuillez consulter Activation de l'outil de recherche d'éléments probants.

En outre, assurez-vous que vous êtes autorisé à effectuer des recherches dans Evidence Finder. Pour un exemple de politique d'autorisation que vous pouvez utiliser, consultezAutoriser les utilisateurs à exécuter des requêtes de recherche dans l'outil de recherche d'éléments probants.

Procédure

Pour rechercher des éléments probants sur la console Audit Manager, procédez comme suit.

1. Exécuter une requête de recherche
2. Arrêter une requête de recherche en cours (facultatif)
3. Modifiez les filtres pour votre requête de recherche (facultatif)

> **Note**
>
> Vous pouvez également utiliser l' CloudTrail API pour interroger vos données de preuve. Pour plus d'informations, consultez StartQueryla référence de AWS CloudTrail l'API. Si vous

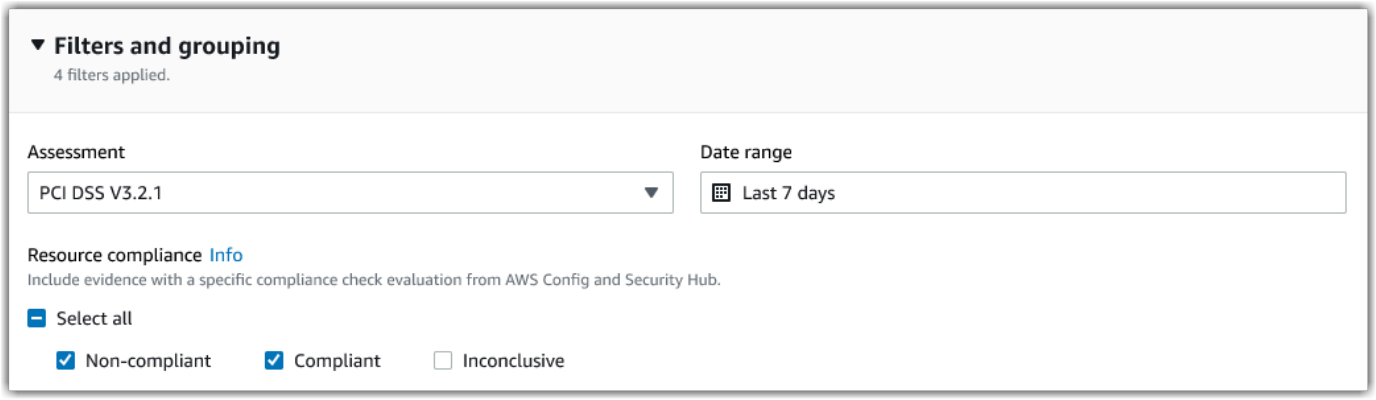
préférez utiliser le AWS CLI, voir Lancer une requête dans le guide de AWS CloudTrail l'utilisateur.

Exécution d'une requête de recherche

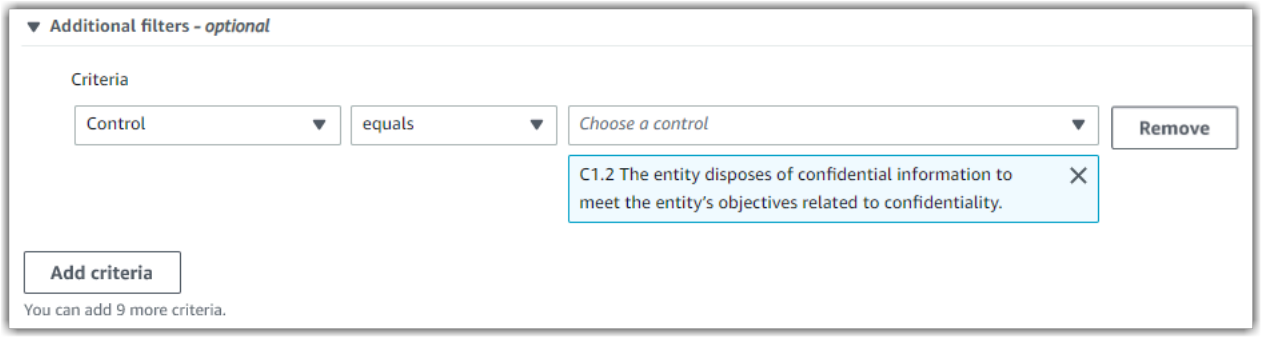
Pour effectuer une requête de recherche dans l'outil de recherche d'éléments probants, procédez comme suit.

Recherchez des éléments probants

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, cliquez sur Outil de recherche d'éléments probants.
3. Puis, appliquez des filtres pour réduire la portée de votre recherche.
   a. Dans Évaluation, choisissez une évaluation.
   b. Dans Plage de dates, sélectionnez une plage.
   c. Dans Conformité des ressources, sélectionnez un statut d'évaluation.



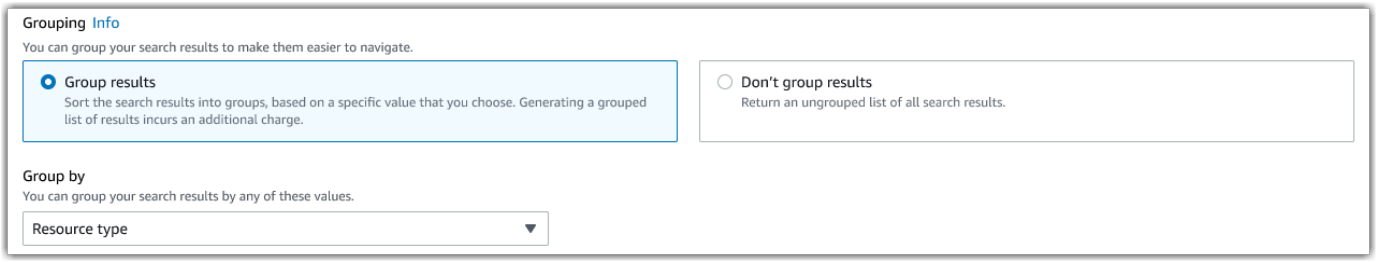
4. (Facultatif) Cliquez sur Filtres supplémentaires - facultatif pour affiner encore davantage la recherche.
   a. Cliquez surAjouter des critères, sélectionnez un critère, puis une ou plusieurs valeurs pour ce critère.
   b. Continuez à créer d'autres filtres de la même manière.
   c. Pour supprimer un filtre indésirable, cliquez sur Supprimer.



5. Sous Regroupement, indiquez si vous souhaitez regrouper les résultats de la recherche.

   a. Si vous souhaitez regrouper les résultats, sélectionnez une valeur selon laquelle les résultats seront regroupés.

   b. Si vous ne souhaitez pas regrouper les résultats, passez à l'étape 6.



6. Choisissez Rechercher.

Votre recherche peut prendre quelques minutes, en fonction du nombre d'éléments probants dont vous disposez. N'hésitez pas à quitter l'outil de recherche d'éléments probants en cours de recherche. Une barre clignotante vous avertit lorsque les résultats de la recherche sont prêts.

Interrompre une requête de recherche

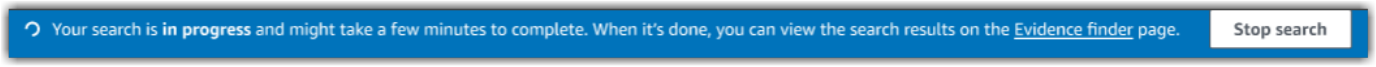
Si vous souhaitez interrompre une requête de recherche, procédez comme suit.

> **Note**
>
> Même si elle est interrompue, une requête de recherche peut entraîner des frais. Le nombre de données d'éléments probants analysés avant l'interruption de la requête de recherche

vous sera facturé. Une fois l'opération interrompue, vous pouvez consulter les résultats partiels renvoyés.

Pour interrompre une requête de recherche en cours

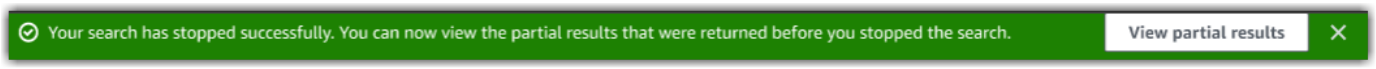
1. Dans la barre de progression bleue située en haut de l'écran, choisissez Arrêter la recherche.



2. (Facultatif) Vérifiez les résultats partiels renvoyés avant l'arrêt de la requête de recherche.

   a. Si vous êtes sur la page de l'outil de recherche d'éléments probants, les résultats partiels s'affichent à l'écran.

   b. Si vous avez quitté l'outil de recherche d'éléments probants, choisissez Afficher les résultats partiels dans la barre de confirmation verte.



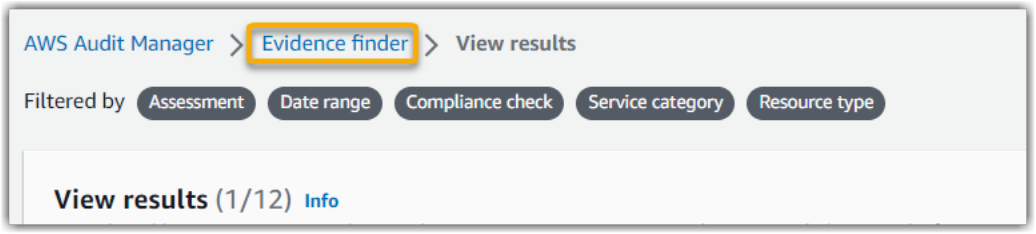
Modification des filtres de recherche

Suivez ces étapes pour revenir à votre dernière requête de recherche et ajuster les filtres selon vos besoins.

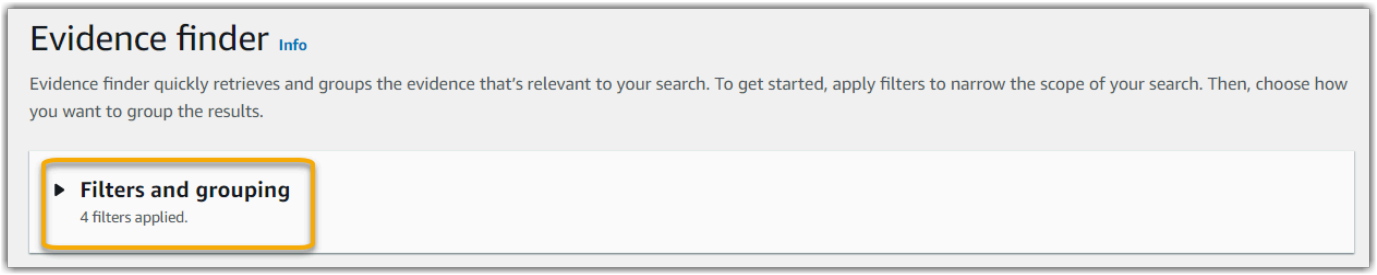
> **Note**
>
> Si vous modifiez les filtres et que vous choisissez Rechercher, une nouvelle requête de recherche est lancée.

Pour modifier une requête de recherche récente

1. Sur la page Afficher les résultats, choisissez Outil de recherche d'éléments probants dans la piste de navigation.



2. Pour développer la sélection de filtres, cliquez sur Filtres et regroupements.



3. Modifiez ensuite vos filtres ou lancez une nouvelle recherche.

   a. Pour modifier les filtres, ajustez ou supprimez les filtres et la sélection de groupes actuels.

   b. Pour recommencer, cliquez sur Effacer les filtres et appliquez les filtres et les regroupements de votre choix.

4. Lorsque vous avez terminé, sélectionnez Recherche.

Étapes suivantes

Une fois votre recherche terminée, vous pouvez consulter les résultats correspondant à vos critères de recherche. Pour obtenir des instructions, veuillez consulter Affichage des résultats dans l'outil de recherche d'éléments probants.

Ressources supplémentaires

- Options de filtrage et de regroupement pour l'outil de recherche de preuves.
- Exemples de cas d'utilisation de l'outil de recherche de preuves.

- Résolution des problèmes liés à l'outil de recherche d'éléments probants.

Affichage des résultats dans l'outil de recherche d'éléments probants

Une fois votre recherche terminée, vous pouvez consulter les résultats correspondant à vos critères de recherche.

N'oubliez pas que plusieurs ressources peuvent être évaluées lors de la collecte d'éléments probants. Par conséquent, ceux-ci peuvent inclure une ou plusieurs ressources connexes. Dans l'outil de recherche d'éléments probants, les résultats s'affichent par ressource, chaque ligne correspondant à une ressource. Vous pouvez prévisualiser un résumé de chaque ressource sans quitter la page.

Après avoir examiné les résultats de la recherche, vous pouvez générer un rapport d'évaluation comprenant ces éléments probants. Vous pouvez également exporter les résultats de votre recherche dans un fichier CSV (valeurs séparées par des virgules).

> **Important**
>
> Nous vous recommandons de laisser l'outil de recherche d'éléments probants ouvert jusqu'à ce que vous ayez fini d'explorer les résultats de la recherche. Si vous quittez le tableau Afficher les résultats, les résultats de votre recherche sont supprimés. Si nécessaire, vous pouvez consulter vos derniers résultats dans la CloudTrail console à l'adresse https://console.aws.amazon.com/cloudtrail/. Les résultats de vos requêtes de recherche y sont conservés pendant sept jours. Cependant, n'oubliez pas que vous ne pouvez pas générer de rapport d'évaluation à partir des résultats de recherche dans la CloudTrail console.

Prérequis

La procédure suivante suppose que vous avez déjà suivi les étapes pour effectuer une recherche dans Evidence Finder.

Procédure

Suivez ces étapes pour afficher les résultats de votre recherche dans Evidence Finder.

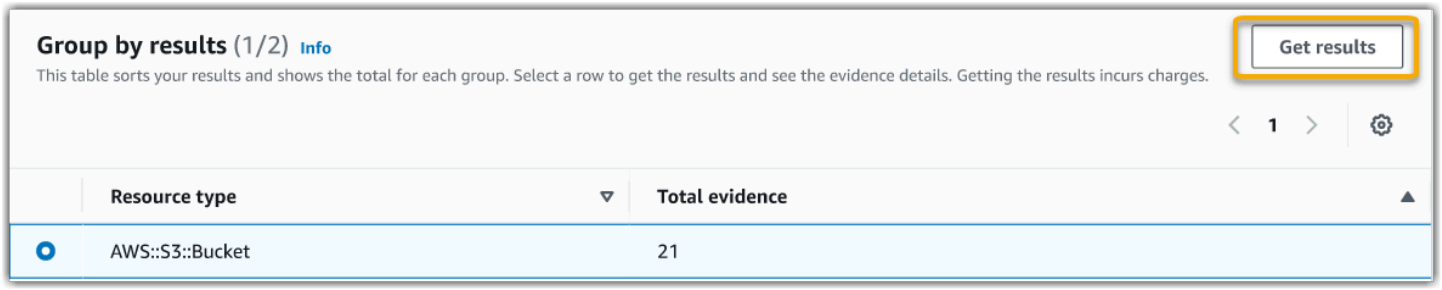
Tâches

Étape 1. Affichage des résultats groupés

Si vous avez regroupé vos résultats, vous pouvez passer en revue ces regroupements avant d'analyser plus en profondeur les éléments probants.

> **Note**
>
> Si vous n'avez pas regroupé les résultats, l'outil de recherche d'éléments probants n'affiche pas le tableau Regrouper par résultats. Au lieu de cela, vous êtes redirigé directement vers le tableau Afficher les résultats.

Le tableau Regrouper par résultats vous indique l'étendue des éléments probants trouvés et leur répartition spécifique. Les résultats sont regroupés en fonction de la valeur sélectionnée. Par exemple, si vous avez groupé par type de ressource, le tableau affiche une liste des types de AWS ressources. La colonne Total des éléments probants indique le nombre de résultats trouvés pour chaque type de ressource.



Pour obtenir les résultats d'un groupe

1. Dans le tableau Grouper par résultats, sélectionnez la ligne correspondant aux résultats que vous souhaitez obtenir.
2. Cliquez sur Obtenir les résultats. Une nouvelle requête de recherche se lance et vous êtes redirigé vers le tableau Afficher les résultats, où vous pouvez voir les résultats du groupe désiré.

Étape 2. Affichage des résultats de la recherche

Le tableau Afficher les résultats affiche les résultats de votre recherche. À partir de là, vous pouvez gérer vos préférences d'affichage et prévisualiser les résumés des ressources.

Gestion de vos préférences de visionnage

Vos préférences d'affichage contrôlent ce que vous voyez sur la page des résultats.

Pour gérer vos préférences d'affichage

1. Cliquez sur l'icône des paramètres (#) en haut du tableau Afficher les résultats.
2. Vérifiez et modifiez les paramètres suivants au besoin :

Paramètre	Description
Sélectionnez les colonnes visibles du tableau	Utilisez l'option de bascule pour modifier les colonnes affichées.
Taille de page	Sélectionnez un bouton radio pour spécifier le nombre de résultats affichés sur chaque page.
Wrap text (Retour à la ligne)	Cochez la case pour enrouler de longues lignes de texte afin d'en améliorer la lisibilité.

3. Choisissez Confirmer pour enregistrer vos préférences.

Afficher un aperçu des résumés des ressources

Vous pouvez prévisualiser les ressources associées aux éléments probants correspondant à votre requête de recherche. Cela vous permet de déterminer si la requête de recherche a renvoyé les résultats escomptés ou si vous devez ajuster vos filtres et réexécuter celle-ci.

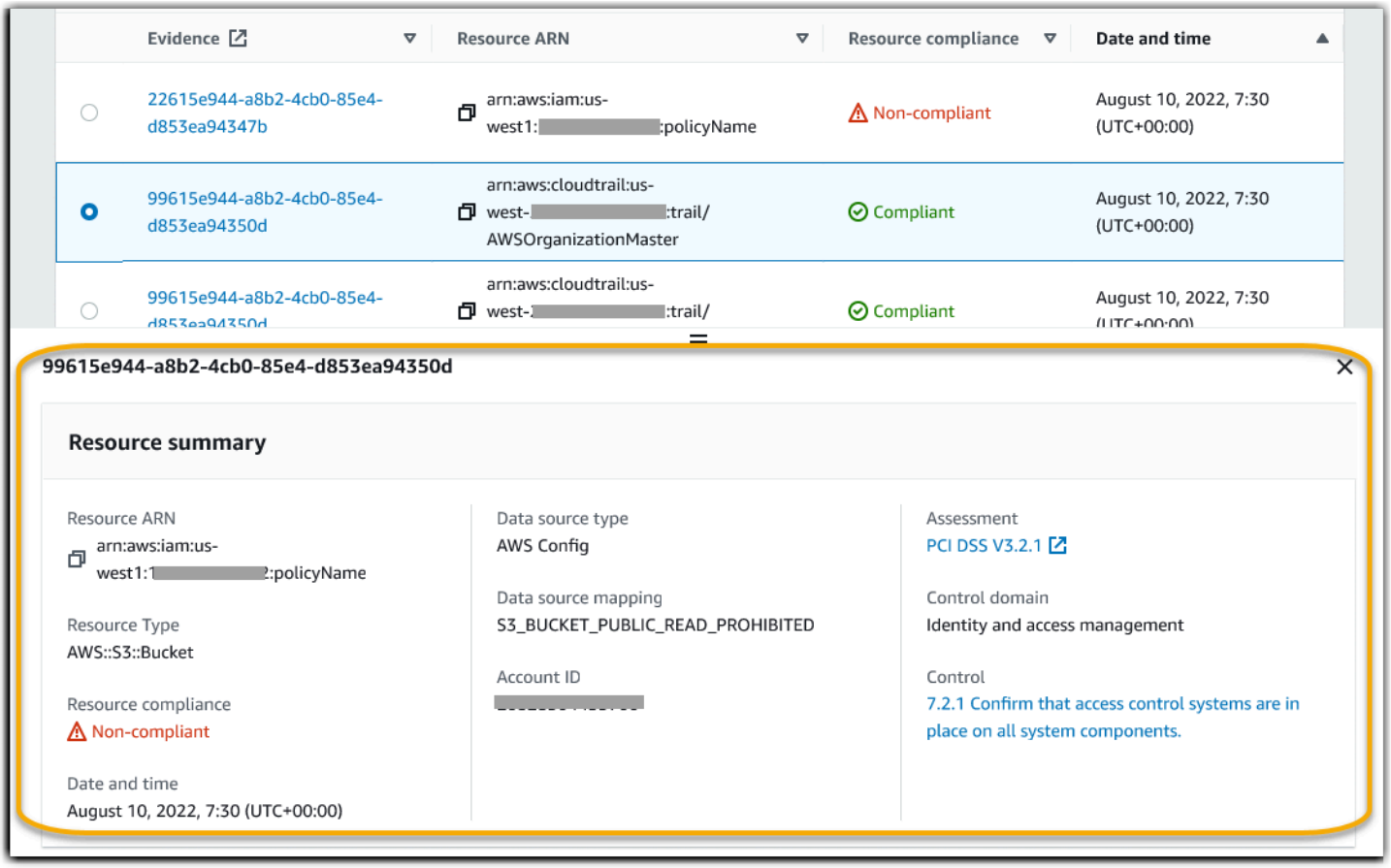
N'oubliez pas que les éléments probants peuvent avoir une ou plusieurs ressources connexes. L'outil de recherche d'éléments probants affiche les résultats par ressources (une ligne par ressource).

> **Note**
>
> L'outil de recherche d'éléments probants renvoie des résultats d'éléments probants automatisés ou manuels. Toutefois, vous ne pouvez prévisualiser les récapitulatifs des

ressources que pour les éléments probants automatisés. Cela est dû au fait qu'Audit Manager n'évalue pas les ressources pour les éléments probants manuels et que, par conséquent, aucun résumé des ressources n'est disponible.
Pour voir le détail d'un élément probant manuel, cliquez sur son nom : la page détaillée s'ouvre. Si vous générez un rapport d'évaluation à partir des résultats de votre recherche d'éléments probants, le détail de ceux-ci sera inclus dans le rapport d'évaluation.

Pour prévisualiser les récapitulatifs de ressources

1. Activez la case d'option située en regard d'un résultat. Un panneau récapitulatif des ressources s'ouvre sur la page en cours.
2. (Facultatif) Pour voir le détail de l'élément probant connexe, cliquez sur son nom.
3. (Facultatif) Utilisez les lignes horizontales (=) pour faire glisser et redimensionner le volet récapitulatif des ressources.
4. Cliquez sur (x) pour fermer le volet récapitulatif des ressources.



Étapes suivantes

Après avoir examiné les résultats de recherche, vous pouvez générer un rapport d'évaluation à partir de ceux-ci ou les exporter sous forme de fichier CSV. Pour obtenir des instructions, veuillez consulter Exporter les résultats de votre recherche depuis Evidence Finder.

Ressources supplémentaires

- Options de filtrage et de regroupement pour l'outil de recherche de preuves
- Exemples de cas d'utilisation de l'outil de recherche de preuves
- Résolution des problèmes liés à l'outil de recherche d'éléments probants

Exporter les résultats de votre recherche depuis Evidence Finder

Après avoir examiné les résultats de votre recherche, vous pouvez générer un rapport d'évaluation basé sur ces résultats. Vous pouvez également exporter les résultats de votre recherche de preuves dans un fichier CSV.

Prérequis

La procédure suivante suppose que vous avez déjà suivi les étapes pour effectuer une recherche et passer en revue les résultats de votre recherche dans Evidence Finder.

Procédure

Table des matières

Génération d'un rapport d'évaluation à partir des résultats de votre recherche

Une fois que vous êtes satisfait des résultats de recherche, vous pouvez générer un rapport d'évaluation.

Générer un rapport d'évaluation à partir des résultats de votre recherche

1. En haut du tableau Afficher les résultats, sélectionnez Générer un rapport d'évaluation.
2. Entrez un nom et une description pour votre rapport d'évaluation, puis passez en revue ses détails.
3. Choisissez Générer un rapport d'évaluation.

Votre rapport d'évaluation est généré en l'espace de quelques minutes. Vous pouvez, pendant ce temps ; quitter l'outil de recherche d'éléments probants : une notification verte de réussite confirmera que le rapport est prêt. Vous pouvez ensuite accéder au centre de téléchargement d'Audit Manager et télécharger votre rapport d'évaluation.

> **Note**
>
> Audit Manager génère un rapport unique à partir des éléments probants des résultats de recherche uniquement. Ce rapport ne comprend aucun élément probant ajouté manuellement à un rapport sur la page d'évaluation.
> Des limites s'appliquent au nombre d'éléments probants pouvant être inclus dans un rapport d'évaluation. Pour plus d'informations, consultez Résolution des problèmes liés à l'outil de recherche d'éléments probants.

Exportation des résultats de recherche dans un fichier CSV

Vous pourrez avoir besoin d'une version portable des résultats de votre recherche. Dans ce cas, vous pouvez exporter les résultats de votre recherche dans un fichier CSV.

Une fois les résultats de votre recherche exportés, le fichier CSV sera disponible dans le centre de téléchargement d'Audit Manager pendant sept jours. Une copie de ce fichier CSV sera également envoyée vers votre compartiment S3 préféré, la destination d'exportation. Votre fichier CSV restera disponible dans ce compartiment jusqu'à ce que vous le supprimiez.

Audit Manager utilise la fonctionnalité CloudTrail Lake pour exporter et diffuser des fichiers CSV depuis Evidence Finder. Les facteurs suivants définissent le fonctionnement du processus d'exportation au format CSV :

- Tous les résultats de votre recherche sont inclus dans le fichier CSV. Si vous souhaitez uniquement inclure des résultats de recherche spécifiques, nous vous recommandons de modifier

vos filtres de recherche. Ainsi, vous pouvez affiner vos résultats pour cibler uniquement les éléments probants que vous souhaitez exporter.

- Les fichiers CSV sont exportés au format GZIP compressé. Le nom du fichier CSV par défaut est `queryID/result.csv.gz`, `queryID` étant l'ID de votre requête de recherche.
- La taille maximale d'un fichier CSV d'exportation est de 1 To. Si vous exportez plus de 1 To de données, vos résultats seront répartis dans plusieurs fichiers. Chaque fichier CSV est nommé `result_number.csv.gz`. Le nombre de fichiers CSV obtenu dépend de la taille totale des résultats de la recherche. Par exemple, l'exportation de 2 To de données vous fournit deux fichiers de résultats de requête : `result_1.csv.gz` et`result_2.csv.gz`.
- Outre le fichier CSV, un fichier de signature JSON est envoyé à votre compartiment S3. Ce fichier agit comme une somme de contrôle pour vérifier l'exactitude des informations contenues dans le fichier CSV. Pour en savoir plus, consultez la structure des fichiers de CloudTrail signature dans le Guide du AWS CloudTrail développeur. Pour déterminer si les résultats de la requête ont été modifiés, supprimés ou inchangés après leur livraison, vous pouvez utiliser la validation de l'intégrité des résultats de la CloudTrail requête. Pour des instructions détaillées, consultez la section Valider les résultats des requêtes enregistrées du Guide du développeur AWS CloudTrail .

> **Note**
>
> Les réponses textuelles des éléments probants manuels ne sont actuellement pas comprises dans les aperçus de l'outil de recherche d'éléments probants, ni dans les exportations CSV. Pour voir les données de réponse textuelle, choisissez le nom d'élément probant manuel dans les résultats de votre outil de recherche d'éléments probants pour ouvrir leur page détaillée. Si vous devez consulter les données des réponses textuelles en dehors de la console Audit Manager, nous vous recommandons de générer un rapport d'évaluation à partir des résultats de votre recherche d'éléments probants. Tous les détails relatifs aux éléments probants manuels, y compris les réponses textuelles, sont inclus dans les rapports d'évaluation.

Exporter vos résultats pour la première fois

Pour exporter les résultats de votre recherche pour la première fois, procédez comme suit. Cette procédure vous permet de définir une destination d'exportation par défaut pour toutes vos futures exportations. Si vous ne souhaitez pas enregistrer de destination d'exportation par défaut pour

le moment, vous pouvez le faire ultérieurement en mettant à jour vos paramètres de destination d'exportation.

> **Important**
>
> Avant de commencer, assurez-vous que vous disposez d'un compartiment S3 comme destination d'exportation. Vous pouvez utiliser l'un de vos compartiments S3 existants ou créer un nouveau compartiment dans Amazon S3. En outre, votre compartiment S3 doit disposer de la politique d'autorisation requise pour CloudTrail permettre d'y écrire les fichiers d'exportation. Plus précisément, la politique de compartiment doit inclure une `s3:PutObject` action et l'ARN du compartiment, et la liste CloudTrail en tant que principal de service. Nous fournissons un exemple de politique d'autorisation que vous pouvez utiliser. Pour savoir comment joindre cette politique à votre compartiment S3, consultez Ajout d'une stratégie de compartiment à l'aide de la console Amazon S3.
> Pour plus de conseils, consultezConseils de configuration pour votre destination d'exportation. Si vous rencontrez des problèmes lors de l'exportation d'un fichier CSV, consultezcsv-exports.

Pour exporter les résultats de votre recherche (première fois)

1. En haut du tableau Afficher les résultats, sélectionnez Exporter au format CSV.
2. Précisez le compartiment S3 vers lequel vous souhaitez exporter vos fichiers.
   - Choisissez Parcourir S3 pour sélectionner un compartiment dans la liste.
   - Vous pouvez également saisir l'URI du compartiment au format suivant : **`s3://bucketname/prefix`**

   > **Tip**
   >
   > Pour que votre compartiment de destination reste organisé, vous pouvez créer un dossier facultatif pour vos exportations CSV. Pour ce faire, ajoutez une barre oblique (**`/`**) et un préfixe à la valeur dans la zone URI de ressource (par exemple, **`/evidenceFinderExports`**). Audit Manager ajoutera alors ce préfixe lors de l'envoi du fichier CSV au compartiment et Amazon S3 génèrera le chemin spécifié par le préfixe. Pour plus d'informations sur les préfixes dans Amazon S3, veuillez consulter

Organisation des objets dans la console Amazon S3 dans le Guide de l'utilisateur Amazon Simple Storage Service.

3. (Facultatif) Si vous ne souhaitez pas enregistrer ce compartiment comme destination d'exportation par défaut, décochez la case Enregistrer ce compartiment comme destination d'exportation par défaut dans les paramètres de mon outil de recherche d'éléments probants.
4. Cliquez sur Exporter.

Exporter vos résultats après avoir enregistré une destination d'exportation

Une fois votre compartiment S3 enregistré comme destination d'exportation par défaut, vous pouvez procéder comme suit.

Pour exporter les résultats de votre recherche (après avoir enregistré une destination d'exportation par défaut)

1. En haut du tableau Afficher les résultats, sélectionnez Exporter au format CSV.
2. Dans l'invite qui s'affiche, vérifiez le compartiment S3 par défaut dans lequel votre fichier exporté sera enregistré.
   a. (Facultatif) Pour continuer à utiliser ce compartiment et masquer ce message à l'avenir, cochez la case Ne plus me le rappeler.
   b. (Facultatif) Pour changer de compartiment, suivez la procédure de mise à jour de vos paramètres de destination d'exportation.
3. Choisissez Confirmer.

En fonction de la quantité de données que vous exportez, le processus d'exportation peut prendre quelques minutes. N'hésitez pas à quitter l'outil de recherche d'éléments probants pendant que l'exportation est en cours d'exécution. Si vous quittez l'outil de recherche d'éléments probants, votre recherche sera interrompue et les résultats de recherche seront ignorés dans la console. Toutefois, le processus d'exportation CSV se poursuit en arrière-plan. Le fichier CSV contiendra l'ensemble complet des résultats de recherche correspondant à votre requête.

Afficher vos résultats une fois exportés

Pour trouver votre fichier CSV et vérifier son statut, rendez-vous dans l'Audit ManagerCentre de téléchargement d'Audit Manager. Lorsque le fichier exporté est prêt, vous pouvez télécharger votre fichier CSV depuis le centre de téléchargement.

Vous pouvez également rechercher et télécharger le fichier CSV depuis votre compartiment S3 de destination d'exportation.

Pour rechercher votre fichier CSV et votre fichier de signature dans la console Amazon S3

1. Ouvrez la console Amazon S3.
2. Choisissez le compartiment de destination d'exportation que vous avez indiqué lors de l'exportation de votre fichier CSV.
3. Parcourez la hiérarchie des objets jusqu'à ce que vous trouviez le fichier CSV et le fichier de signature. Le fichier CSV a une extension `.csv.gz` et le fichier de signature une extension `.json`.

Vous allez parcourir une hiérarchie d'objets similaire à l'exemple suivant, mais avec un nom de compartiment de destination d'exportation, un ID de compte, une date et un ID de requête différents.

```
All Buckets
    Export_Destination_Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        YYYY
                            MM
                              DD
                                Query_ID
```

Ressources supplémentaires

- Résolution des problèmes liés à l'outil de recherche d'éléments probants
- Configuration de votre destination d'exportation par défaut pour Evidence Finder

Options de filtrage et de regroupement pour l'outil de recherche de preuves

Sur cette page, vous pouvez voir une liste des options de filtre et de regroupement que vous pouvez utiliser dans Evidence Finder.

Référence du filtre

Vous pouvez utiliser les filtres suivants pour trouver des preuves correspondant à des critères spécifiques, tels qu'une évaluation, un contrôle ou Service AWS.

Rubriques

Filtres requis

Ces filtres vous donneront un aperçu général des éléments probants d'une évaluation pour commencer.

Nom du filtre	Description	Remarques
Évaluation	Renvoie des éléments probants pour une évaluation spécifique.	Vous pouvez filtrer en fonction d'une seule évaluation.
Plage de dates	Renvoie des éléments probants pour une période donnée.	Vous pouvez utiliser soit une plage relative, pour définir une plage de date du jour (par exemple, **`Last 30 days`**). soit une plage absolue pour spécifier une plage de dates spécifique (par exemple, **`June 27th - July 4th`**).

Nom du filtre	Description	Remarques
Conformité des ressources	Renvoie les ressources avec une évaluation de vérification de conformité spécifique.	Audit Manager collecte des preuves de conformité pour les contrôles qui utilisent AWS Config Security Hub comme type de source de données. Plusieurs ressources peuvent être évaluées pour la collecte d'éléments probants. Par conséquent, un même élément probant pour la vérification de conformité peut comprendre une ou plusieurs ressources. Vous pouvez utiliser ce filtre pour explorer l'état de conformité par ressources. Vous pouvez choisir l'une ou plusieurs options parmi les options suivantes : • Non conforme : ce filtre trouve les ressources présentant des problèmes lors de la vérification de conformité. Cela se produit si Security Hub signale un résultat d'échec ou un résultat non conforme. AWS Config • Conforme : ce filtre trouve les ressources ne présentant pas de problèmes en termes de conformité. Cela se produit si Security Hub signale un résultat de réussite ou un résultat conforme. AWS Config • Non concluant : ce filtre trouve les ressources pour lesquelles aucune vérification de conformité n'est disponible ou applicable. Cela se produit si une ressource utilise AWS Config ou Security Hub comme type de source de données sous-jacent, mais que ces services ne sont pas activés. Cela se produit également si la ressource utilise un type de source de données sous-jacent qui ne prend pas en charge les contrôles de conformité (tels que les preuves

Nom du filtre	Description	Remarques
		manuelles, les appels d' AWS API ou CloudTrail).

Filtres supplémentaires (en option)

Utilisez ces filtres pour affiner la portée de votre requête de recherche. Par exemple, utilisez Service pour voir tous les éléments probants liés à Amazon S3. Utilisez Type de ressource pour vous limiter aux compartiments S3. Vous pouvez également utiliser Ressource ARN pour cibler un compartiment S3 spécifique.

Vous pouvez créer des filtres supplémentaires en utilisant un ou plusieurs des critères suivants.

Nom du critère	Description	Quand utiliser ce critère
ID de compte	Profilez vers le bas par Compte AWS.	Utilisez ce critère pour trouver des éléments probants liés à un Compte AWS spécifique.
Contrôle	Explorer par nom de contrôle.	Utilisez ce critère pour trouver des éléments probants liés à un contrôle spécifique.
Domaine de contrôle	Explorer par domaine de contrôle.	Utilisez ce critère pour vous limiter à un domaine spécifique pour la préparation d'un audit. Vous pouvez filtrer par domaine de contrôle si vous interrogez une évaluation créée à partir d'un framework standard. Les domaines de contrôle peuvent être, par exemple, la gestion des identités et des accès, la journalisation et la surveillance, ou la gestion du réseau.
Data source type (Type de source	Explorer par type de source de données.	Utilisez ce critère pour vous limiter à une source de données spécifique. Définissez la valeur sur `Manual` pour rechercher les éléments probants envoyés manuellement. Sinon, vous

Nom du critère	Description	Quand utiliser ce critère
de données)		pouvez filtrer les éléments probants automatisés en fonction de leur provenance (par exemple `AWS Config`, `CloudTrail` , `Security Hub`, ou`AWS API calls`).
Nom de l'événement	Explorer par nom d'événement.	Utilisez ce critère pour vous limiter à un événement spécifique auquel les éléments probants sont liés. Un événement est l'enregistrement d'une activité dans un Compte AWS. Par exemple, vous pouvez rechercher le nom d'un appel d'API, comme l'opération IAM `AttachRolePolicy` utilisée pour configurer les autorisations. Vous pouvez également rechercher un CloudTrail mot clé, tel que l'`ConsoleLogin` événement enregistré CloudTrail lorsqu'un utilisateur se connecte à votre compte.
ARN des ressources	Explorer par Amazon Resource Name (ARN).	Utilisez ce critère pour trouver des éléments probants liés à une ressource AWS spécifique.
Type de ressource	Explorer par type de ressource.	Utilisez ce critère pour vous limiter au type de ressource évalué, comme une instance Amazon EC2 ou un compartiment S3.
Service	Effectuez une recherche par Service AWS nom.	Utilisez ces critères pour trouver des preuves liées à un élément spécifique Service AWS, tel qu'Amazon EC2, Amazon S3 ou. AWS Config
Catégorie de services	Profilez par Service AWS catégorie.	Utilisez ces critères pour vous concentrer sur une catégorie spécifique de Service AWS. Par exemple la sécurité, l'identité et la conformité, les bases de données et le stockage.

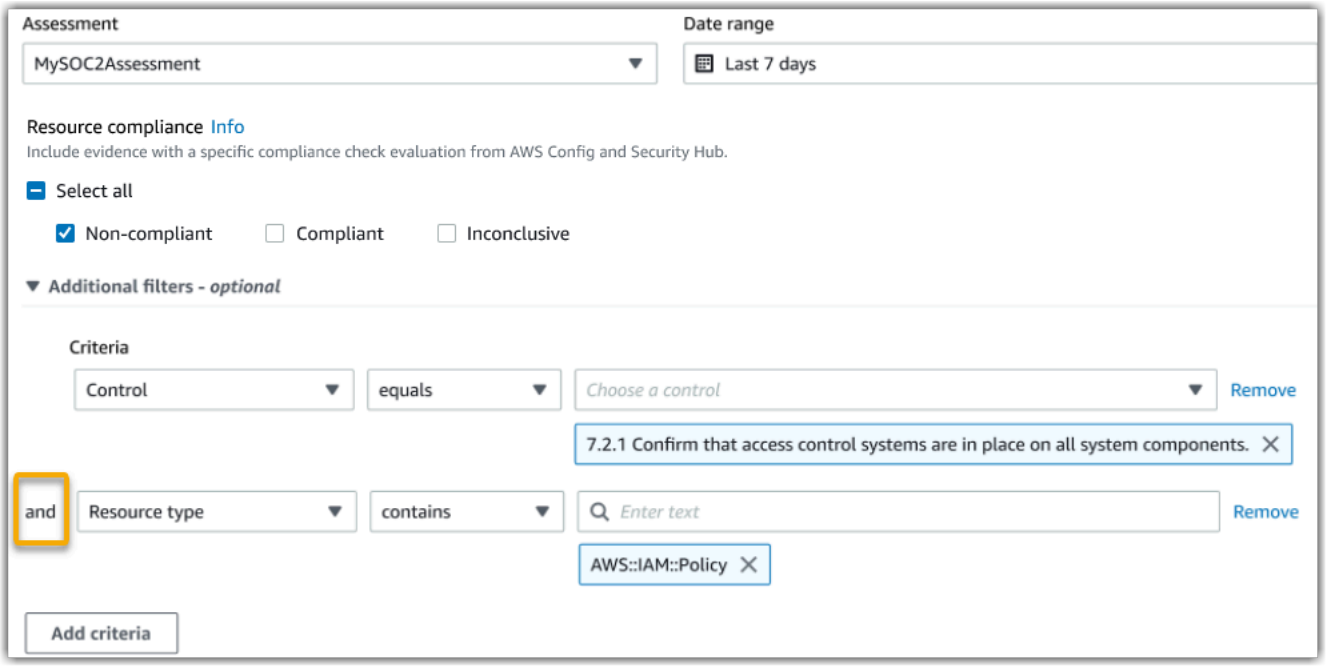
Filtres multiples

Comportement des critères

Si vous spécifiez plusieurs critères, Audit Manager applique l'opérateur AND à vos sélections. Cela signifie que tous les critères sont regroupés dans une seule requête et que les résultats doivent correspondre à tous les critères conjugués.

Exemple

Dans la configuration de filtre suivante, l'outil de recherche d'éléments probants renvoie les ressources non conformes des 7 derniers jours pour l'évaluation dénommée **`MySOC2Assessment`**. En outre, les résultats concernent à la fois une politique IAM et le contrôle spécifié.

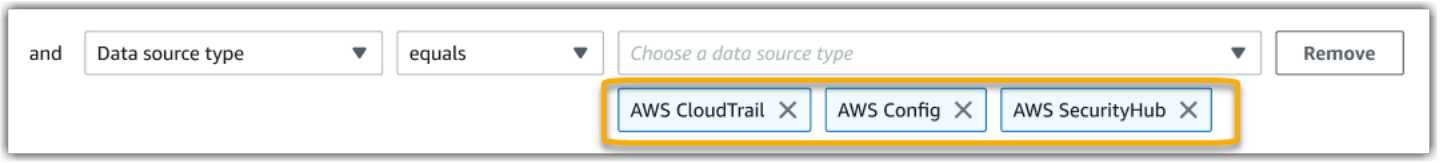


Comportement des valeurs de critère

Si vous spécifiez plusieurs valeurs de critère, ces valeurs sont liées par un opérateur OR. L'outil de recherche d'éléments probants renvoie des résultats correspondant à l'une de ces valeurs de critères.

Exemple

Dans la configuration de filtre suivante, Evidence Finder renvoie des résultats de recherche provenant soit de AWS CloudTrail AWS Config, soit AWS Security Hub.



Référence de regroupement

Vous pouvez regrouper les résultats de recherche pour accélérer la navigation. Le regroupement vous montre l'étendue de vos résultats de recherche et leur répartition spécifique.

Vous pouvez utiliser le regroupement par les valeurs suivantes de votre choix.

Regrouper par	Description
ID de compte	Regrouper les résultats par Compte AWS.
Contrôle	Regroupez les résultats par nom de contrôle.
Data source type (Type de source de données)	Regroupez les résultats par type de source de données d'où proviennent les éléments probants.
Nom de l'événement	Regroupez les résultats par nom d'événement.
ARN des ressources	Regroupez les résultats par Amazon Resource Name (ARN).
Type de ressource	Regroupez les résultats par type de ressource.
Service	Regroupez les résultats par Service AWS nom.
Catégorie de services	Regroupez les résultats par Service AWS catégorie.

Exemples de cas d'utilisation de l'outil de recherche de preuves

L'outil de recherche d'éléments probants peut vous aider dans plusieurs cas d'utilisation. Cette page fournit quelques exemples et suggère les filtres de recherche que vous pouvez utiliser dans chaque scénario.

Rubriques

Cas d'utilisation 1 : trouver des éléments probants non conformes et organiser des délégations

Ce cas d'utilisation est idéal si vous êtes responsable de la conformité ou de la protection des données ou un professionnel GRC chargé de superviser la préparation des audits.

Pour la surveillance du niveau de conformité de votre organisation, vous pouvez compter sur vos équipes partenaires pour vous aider à résoudre les problèmes. L'outil de recherche d'éléments probants vous aide à organiser votre travail pour vos équipes partenaires.

En appliquant des filtres, vous pouvez vous limiter aux éléments probants d'un seul domaine à la fois. De plus, vous pouvez également rester en phase avec les responsabilités et le champ d'action de chaque équipe partenaire avec laquelle vous travaillez. En effectuant une recherche ciblée de cette manière, vous pouvez utiliser les résultats de recherche pour identifier exactement ce qui doit être corrigé dans chaque domaine. Vous pouvez ensuite déléguer ces éléments probants non conformes à l'équipe partenaire correspondante pour qu'elle y remédie.

Pour ce flux de travail, procédez à la recherche d'éléments probants. Utilisez les filtres suivants pour rechercher des éléments probants de non-conformité.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Non-compliant
```

Appliquez ensuite des filtres supplémentaires pour le domaine choisi. Par exemple, utilisez le filtre Catégorie de service pour rechercher les ressources non conformes liées à IAM. Partagez ensuite ces résultats avec l'équipe responsable des ressources IAM de votre organisation. Ou si vous interrogez une évaluation créée à partir d'un framework standard, vous pouvez utiliser le filtre Domaine de contrôle pour trouver des éléments probants de non-conformité liées au domaine de gestion des identités et des accès.

```
Control domain | <domain that you're focusing on>
or
```

```
Service category | <Service AWS category that you're focusing on>
```

Une fois que vous avez trouvé les preuves dont vous avez besoin, suivez les étapes pour générer un rapport d'évaluation à partir des résultats de votre recherche. Pour obtenir des instructions, veuillez consulter Génération d'un rapport d'évaluation à partir des résultats de votre recherche. Vous pouvez partager ce rapport avec votre équipe partenaire, qui pourra l'utiliser comme liste de contrôle des mesures correctives.

Cas d'utilisation 2 : Identification des éléments probants de conformité

Ce cas d'utilisation est idéal si vous travaillez dans SecOps un rôle informatique ou si vous DevOps occupez un autre poste qui possède et corrige les actifs du cloud.

Dans le cadre d'un audit, il peut vous être demandé de résoudre des problèmes liés aux ressources dont vous êtes responsable. Une fois de travail effectué, vous pouvez valider la conformité de vos ressources à l'aide de l'outil de recherche d'éléments probants.

Pour ce flux de travail, procédez à la recherche d'éléments probants. Utilisez les filtres suivants pour rechercher des éléments probants de conformité.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Compliant
```

Puis, appliquez des filtres supplémentaires pour n'afficher que les éléments probants dont vous êtes responsable. Selon l'étendue de votre responsabilité, faites en sorte que la recherche soit aussi ciblée que nécessaire. Les exemples de filtres suivants vont du plus large au plus précis. Choisissez les options qui vous conviennent et remplacez-les *<placeholder text>* par vos propres valeurs.

```
Control domain | <a subject area that you're responsible for>
Service category | <a category of Services AWS that you own>
Service | <a specific Service AWS that you own>
Resource type | <a collection of resources that you own>
Resource ARN | <a specific resource that you own>
```

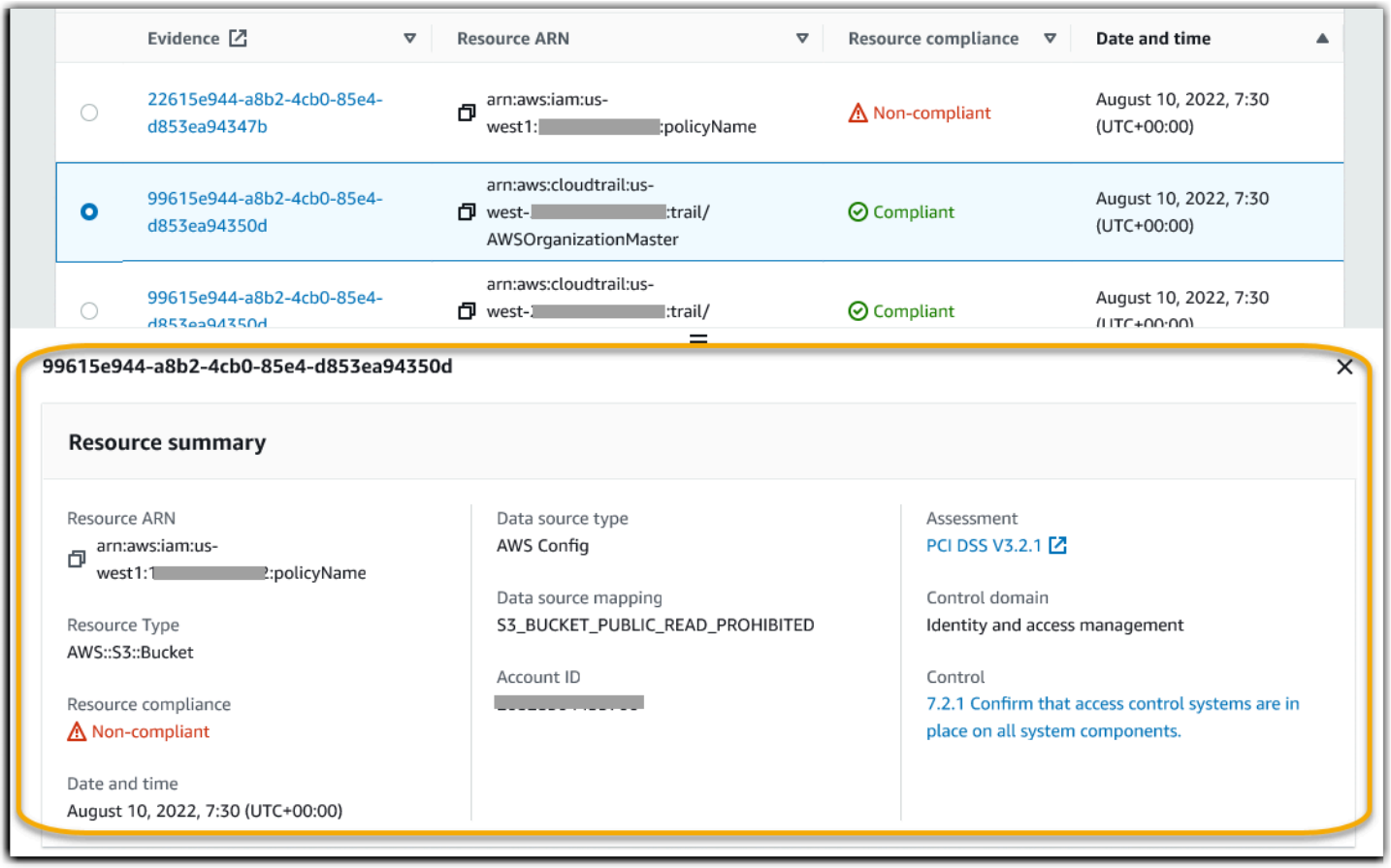
Si vous êtes responsable de plusieurs instances des mêmes critères (par exemple, vous en possédez plusieurs Services AWS), vous pouvez regrouper vos résultats en fonction de cette valeur. Cela vous fournit le total des éléments probants concordants pour chaque Service AWS. Vous pouvez ensuite obtenir les résultats pour les services dont vous êtes responsable.

Cas d'utilisation 3 : aperçu rapide des ressources d'éléments probants

Ce cas d'utilisation est idéal pour tous les clients d'Audit Manager.

Auparavant, l'examen détaillé des éléments probants individuels prenait beaucoup de temps. Si vous vouliez avoir un aperçu des éléments probants, vous deviez accéder directement à cette évaluation, puis parcourir des dossiers d'éléments probants profondément enfouis et difficiles à trouver. Désormais, l'outil de recherche d'éléments probants est un moyen pratique de prévisualiser ces informations. Pour chaque élément probant correspondant à votre requête de recherche, vous pouvez prévisualiser les ressources individuelles correspondantes.

Pour commencer, lancez une recherche d'éléments probants. Activez ensuite la case d'option en regard d'un résultat pour afficher le récapitulatif des ressources dans la page actuelle. Vous pouvez prévisualiser chaque ressource individuelle associée à un élément probant. Pour voir le détail complet des éléments probants de la ressource de votre choix, cliquez sur le nom de cet élément probant. Pour plus d'informations, consultez Afficher un aperçu des résumés des ressources.



Centre de téléchargement d'Audit Manager

Le centre de téléchargement est l'endroit où vous pouvez trouver et gérer tous vos fichiers Audit Manager téléchargeables. Lorsque vous générez un rapport d'évaluation ou que vous exportez des résultats de recherche depuis Outil de recherche d'éléments probants, les fichiers apparaissent dans le centre de téléchargement.

Table des matières

Naviguer dans le centre de téléchargement

Suivez ces étapes pour parcourir vos fichiers dans le centre de téléchargement.

Pour rechercher des fichiers dans le centre de téléchargement

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, sélectionnez Centre de téléchargement.
3. Choisissez l'onglet Rapports d'évaluation pour afficher les rapports d'évaluation disponibles au téléchargement.

   - Cet onglet affiche les rapports d'évaluation que vous avez générés. Les rapports d'évaluation restent disponibles dans le centre de téléchargement jusqu'à ce que vous les supprimiez.
   - Pour voir le statut le plus récent de votre rapport d'évaluation, cliquez sur l'icône d'actualisation (#) pour recharger le tableau. Chaque ligne du tableau des rapports d'évaluation indique le nom du rapport, sa date de création et l'un des statuts suivants :

État	Description
En cours	Audit Manager est en train de générer le rapport d'évaluation.

État	Description
Prêt	Le rapport d'évaluation est disponible en téléchargement.
Error (Erreur)	Le rapport d'évaluation n'a pas pu être généré. Dans ce cas, Audit Manager affiche un message décrivant l'erreur. Pour plus d'informations sur la résolution de ces erreurs, consultezRésolution des problèmes liés aux rapports d'évaluation.

4. Cliquez sur l'onglet Exportations pour afficher les exportations CSV disponibles au téléchargement.

   - Cet onglet affiche les résultats de recherche de preuves que vous avez exportés au cours des sept derniers jours. Les fichiers CSV sont supprimés du centre de téléchargement au bout de sept jours, mais ils restent disponibles dans votre compartiment S3 de destination d'exportation. Pour obtenir des instructions sur la façon de trouver une exportation CSV de recherche d'éléments probants dans votre compartiment de destination S3, consultez Afficher vos résultats une fois exportés.
   - Pour voir le statut le plus récent de vos exportations CSV, cliquez sur l'icône d'actualisation (#) pour recharger le tableau. Chaque ligne du tableau des exportations indique le nom du fichier, sa date d'exportation et l'un des statuts suivants :

État	Description
En cours	Audit Manager prépare le fichier CSV.
Prêt	L'exportation a réussi et le fichier est disponible au télécharg ement.
Error (Erreur)	L'exportation a échoué. Dans ce cas, Audit Manager affiche un message décrivant l'erreur. Pour plus d'informations sur la résolution de ces erreurs, consultezcsv-exports.

> **Note**
>
> N'oubliez pas que l'onglet Exports peut également afficher des fichiers CSV pour les requêtes que vous avez exécutées directement dans AWS CloudTrail Lake. Cela inclut les requêtes effectuées dans la CloudTrail console ou à l'aide de l' CloudTrail API. CloudTrail les exportations apparaissent sur cet onglet si vous avez interrogé le magasin de données d'événements d'Audit Manager et que vous avez choisi d'enregistrer les résultats sur Amazon S3.

Téléchargement d'un fichier

Procédez comme suit pour télécharger un fichier depuis le centre de téléchargement.

Pour télécharger un fichier

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, sélectionnez Centre de téléchargement.
3. Choisissez l'onglet Rapports d'évaluation ou l'onglet Exportations.
4. Sélectionnez le fichier que vous souhaitez télécharger, puis choisissez Télécharger.

Pour savoir comment télécharger un fichier directement depuis votre compartiment de destination S3, consultez la section Téléchargement d'un objet dans le guide de l'utilisateur d'Amazon Simple Storage Service (Amazon S3).

Supprimer un fichier

Suivez ces étapes pour supprimer tous les rapports d'évaluation dont vous n'avez plus besoin dans le centre de téléchargement.

> **Note**
>
> La suppression des exportations CSV du centre de téléchargement n'est actuellement pas prise en charge. Les exportations CSV sont automatiquement supprimées du centre de téléchargement au bout de sept jours.

Pour supprimer un rapport d'évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, sélectionnez Centre de téléchargement.
3. Choisissez l'onglet Rapports d'évaluation.
4. Sélectionnez le rapport d'évaluation que vous souhaitez supprimer, puis choisissez Supprimer.

Si vous souhaitez supprimer un rapport d'évaluation ou une exportation CSV depuis votre compartiment de destination S3, nous vous recommandons d'effectuer cette tâche directement dans Amazon S3. Pour obtenir des instructions, consultez la section Supprimer des objets Amazon S3 dans le Guide de l'utilisateur d'Amazon Simple Storage Service (Amazon S3).

Ressources supplémentaires

- Configuration de votre destination d'exportation par défaut pour Evidence Finder
- Configuration de la destination par défaut de votre rapport d'évaluation
- Résolution des problèmes liés aux rapports d'évaluation
- Résolution des problèmes d'exportation au format CSV
- Téléchargement d'un objet depuis Amazon S3
- Suppression d'objets Amazon S3

Utilisation de la bibliothèque de frameworks pour gérer les frameworks dans AWS Audit Manager

Vous pouvez trouver et gérer des frameworks dans la bibliothèque de frameworks dans AWS Audit Manager.

Un framework détermine les contrôles qui sont testés dans un environnement sur une période. Il définit les contrôles et leurs mappages de sources de données pour une norme ou une réglementation de conformité donnée. Il est également utilisé pour structurer et automatiser les évaluations Audit Manager. Vous pouvez utiliser des cadres comme point de départ pour auditer votre Service AWS utilisation et commencer à automatiser la collecte de preuves.

Points clés

Dans la bibliothèque de frameworks, les frameworks sont organisés dans les catégories suivantes.

- Les frameworks standard sont des frameworks prédéfinis que AWS fournit. Ces cadres sont basés sur les AWS meilleures pratiques relatives aux différentes normes et réglementations de conformité, telles que le RGPD et l'HIPAA. Les cadres standard incluent des contrôles organisés en ensembles de contrôles basés sur la norme de conformité ou la réglementation prise en charge par le cadre.

  Vous pouvez consulter le contenu des frameworks standard, mais vous ne pouvez ni les modifier ni les supprimer. Cependant, vous pouvez créer une copie modifiable de n'importe quel framework standard pour en créer un nouveau répondant à vos besoins spécifiques.
- Les frameworks personnalisés sont des frameworks que vous créez. Vous pouvez créer un cadre personnalisé à partir de zéro ou en faisant une copie modifiable d'un cadre existant. Vous pouvez utiliser des frameworks personnalisés pour organiser les contrôles en ensembles de contrôles de manière à répondre à vos exigences spécifiques.

Vous pouvez créer une évaluation à partir d'un framework standard ou personnalisé.

> **Note**
>
> AWS Audit Manager aide à recueillir des preuves pertinentes pour vérifier la conformité aux normes et réglementations de conformité spécifiques. Cependant, il n'évalue pas votre

conformité lui-même. Les preuves collectées par ce biais peuvent AWS Audit Manager donc ne pas inclure toutes les informations relatives à votre AWS utilisation nécessaires aux audits. AWS Audit Manager ne remplace pas un conseiller juridique ou un expert en conformité.

Ressources supplémentaires

Pour créer et gérer des frameworks dans Audit Manager, suivez les procédures décrites ici.

- Trouver les frameworks disponibles dans AWS Audit Manager
- Révision d'un cadre dans AWS Audit Manager
- Création d'un framework personnalisé dans AWS Audit Manager
  - Création d'un cadre personnalisé à partir de zéro dans AWS Audit Manager
  - Création d'une copie modifiable d'un framework existant dans AWS Audit Manager
- Modification d'un framework personnalisé dans AWS Audit Manager
- Suppression d'un framework personnalisé dans AWS Audit Manager
- Partage d'un framework personnalisé dans AWS Audit Manager
  - Concepts et terminologie de partage de frameworks
  - Envoi d'une demande pour partager un framework personnalisé dans AWS Audit Manager
  - Répondre aux demandes de partage dans AWS Audit Manager
  - Supprimer des demandes de partage dans AWS Audit Manager
- Frameworks pris en charge dans AWS Audit Manager

Trouver les frameworks disponibles dans AWS Audit Manager

Vous trouverez tous les frameworks disponibles sur la page de la bibliothèque Framework de la console Audit Manager.

Vous pouvez également consulter tous les frameworks disponibles à l'aide de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour afficher les frameworks. AWS Audit Manager Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Audit Manager console

Pour consulter les frameworks disponibles sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Bibliothèque de frameworks.
3. Choisissez l'onglet Frameworks standard ou Frameworks personnalisés pour parcourir les frameworks standard et personnalisés disponibles.

AWS CLI

Pour consulter les frameworks disponibles dans le AWS CLI

Pour afficher les frameworks dans Audit Manager, utilisez la list-assessment-frameworkscommande et spécifiez un`--framework-type`. Vous pouvez récupérer la liste des frameworks standard. Vous pouvez également récupérer la liste des frameworks personnalisés.

```
aws auditmanager list-assessment-frameworks --framework-type Standard
```

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Audit Manager API

Pour afficher les frameworks disponibles à l'aide de l'API

Utilisez l'ListAssessmentFrameworksopération et spécifiez un FrameworkType. Vous pouvez renvoyer la liste des frameworks standard. Vous pouvez également renvoyer la liste des frameworks personnalisés.

Pour plus d'informations, choisissez l'un des liens précédents pour en lire davantage dans le Guide de référence de l'API AWS Audit Manager . Cela inclut des informations sur la façon d'utiliser le `ListAssessmentFrameworks` fonctionnement et les paramètres dans l'un des SDK spécifiques au langage AWS .

Étapes suivantes

Lorsque vous êtes prêt à explorer les détails d'un framework, suivez les étapes décrites dansRévision d'un cadre dans AWS Audit Manager. Cette page vous guidera à travers les détails du cadre et expliquera les informations que vous y voyez.

Depuis la page de la bibliothèque de cadres, vous pouvez également créer, modifier, supprimer ou partager un cadre personnalisé.

Ressources supplémentaires

Pour des solutions aux problèmes de framework dans Audit Manager, voirRésolution des problèmes liés au framework.

Révision d'un cadre dans AWS Audit Manager

Vous pouvez consulter les détails d'un framework à l'aide de la console Audit Manager, de l'API Audit Manager ou de AWS Command Line Interface (AWS CLI).

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour afficher les frameworks. AWS Audit Manager Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Audit Manager console

Pour consulter les détails du framework sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.

2. Dans le panneau de navigation de gauche, choisissez Bibliothèque de frameworks pour voir la liste des frameworks disponibles.
3. Choisissez l'onglet Frameworks standard ou Frameworks personnalisés pour parcourir les frameworks disponibles.
4. Choisissez le nom du framework pour l'ouvrir.
5. Passez en revue les détails du cadre en utilisant les informations suivantes comme référence.

Section des détails du framework

Cette section fournit une présentation du framework. Dans cette section, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
Description	Une description du cadre, le cas échéant.
Type de cadre	Spécifie si le framework est un framework standard ou un framework personnalisé.
Type de conformité	Norme ou réglementation de conformité prise en charge par le cadre.

Si vous consultez un framework personnalisé, vous pouvez également consulter les informations suivantes :

Name (Nom)	Description
Créé par	Le compte qui a créé le framework personnalisé.
Date de création	Date à laquelle le cadre personnalisé a été créé.
Dernière mise à jour	Date à laquelle ce cadre a été modifié pour la dernière fois.

Onglet Contrôles

Cet onglet répertorie les contrôles du framework, regroupés par ensemble de contrôles. Dans cet onglet, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
Contrôles regroupés par ensemble de contrôles	Cliquez sur l'icône d'arborescence pour voir les contrôles appartenant à chaque ensemble de contrôles.
Type	Spécifie s'il s'agit d'un contrôle standard ou personnalisé.
Sources de données	Spécifie la source de données à partir de laquelle Audit Manager collecte des preuves pour ce contrôle du framework.

Onglet Tags

Cet onglet liste les balises associées au framework. Dans cet onglet, vous pouvez consulter les informations suivantes :

Name (Nom)	Description
Clé	La clé de balise (par exemple, une norme de conformité, une réglementation ou une catégorie).
Valeur	Valeur de balise.

AWS CLI

Pour consulter les détails du framework dans le AWS CLI

1. Pour identifier le framework que vous souhaitez examiner, exécutez la list-assessment-frameworkscommande et spécifiez un`--framework-type`. Vous pouvez récupérer la liste des frameworks standard. Vous pouvez également récupérer la liste des frameworks personnalisés.

   Dans l'exemple suivant, remplacez le *`texte de l'espace réservé`* par `Custom` ou `Standard`.

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom/Standard
   ```

La réponse renvoie une liste de frameworks. Recherchez le framework que vous souhaitez consulter, et prenez note de l'ID du framework et du Amazon Resource Name (ARN).

2. Pour obtenir les détails du framework, exécutez la get-assessment-frameworkcommande et spécifiez le`--framework-id`.

   Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations.

   ```
   aws auditmanager get-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   > **Tip**
   >
   > Les détails du framework sont renvoyés au format JSON. Pour comprendre ces données, consultez la section get-assessment-framework Sortie dans le manuel de référence des AWS CLI commandes.

3. Pour voir les balises d'un framework, utilisez la list-tags-for-resourcecommande et spécifiez le `--resource-arn` pour le framework.

   Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations :

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:assessmentFramework/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Pour plus d'informations sur les balises dans l'Audit Manager, consultez Balisage des ressources AWS Audit Manager.

Audit Manager API

Pour afficher les détails du framework à l'aide de l'API

1. Pour identifier le framework que vous souhaitez examiner, utilisez l'ListAssessmentFrameworksopération et spécifiez un FrameworkType. Vous pouvez renvoyer la liste des frameworks standard. Vous pouvez également renvoyer la liste des frameworks personnalisés.

Pour la réponse, recherchez le framework que vous souhaitez consulter, et prenez note de l'ID du framework et du Amazon Resource Name (ARN).

2. Pour obtenir les détails du framework, utilisez l'GetAssessmentFrameworkopération. Dans la demande, spécifiez le frameworkId que vous avez obtenu à l'étape 1.

> **Tip**
>
> Les détails du framework sont renvoyés au format JSON. Pour comprendre ces données, consultez la section Éléments de GetAssessmentFramework réponse dans la référence de l'AWS Audit Manager API.

3. Pour voir les balises du framework, utilisez l'ListTagsForResourceopération. Dans la demande, spécifiez le resourceArn du framework que vous avez obtenu à l'étape 1.

Pour plus d'informations sur les balises dans Audit Manager, consultez la section AWS Audit Manager Ressources de balisage.

Pour plus d'informations sur ces opérations d'API, cliquez sur l'un des liens de la procédure précédente pour en savoir plus dans la référence des AWS Audit Manager API. Cela inclut des informations sur la façon d'utiliser ces opérations et paramètres dans l'un des SDK spécifiques au langage AWS .

Étapes suivantes

Sur la page de détails du cadre, vous pouvez créer une évaluation à partir du cadre ou créer une copie modifiable du cadre.

Si vous examinez un cadre personnalisé, vous pouvez également le modifier, le supprimer ou le partager.

Ressources supplémentaires

- Sur la page de détails de mon framework personnalisé, je suis invité à recréer mon framework personnalisé
- Je ne parviens pas à faire une copie de mon framework personnalisé ni à l'utiliser pour créer une évaluation

Création d'un framework personnalisé dans AWS Audit Manager

Vous pouvez utiliser des frameworks personnalisés pour organiser les contrôles en ensembles de contrôles de manière à répondre à vos exigences spécifiques.

Points clés

Pour créer des frameworks personnalisés dans Audit Manager, vous avez le choix entre deux méthodes :

1. Création d'un cadre personnalisé à partir de zéro - Cela vous donne la flexibilité de partir de zéro et de définir chaque aspect du cadre selon vos spécifications. Cette approche est particulièrement avantageuse lorsque vos exigences s'écartent considérablement des cadres standard existants ou lorsque vous devez intégrer des ensembles de contrôle propriétaires spécifiques à votre organisation.
2. Création d'une copie modifiable d'un framework existant - Cette approche vous permet de tirer parti de la structure et du contenu d'un framework existant tout en vous laissant la liberté de le personnaliser en fonction de vos besoins spécifiques. En partant d'une base bien établie, vous pouvez rationaliser le processus de création de votre cadre personnalisé, en concentrant vos efforts sur son adaptation aux exigences uniques de votre organisation.

Quelle que soit l'approche choisie, la création d'une structure personnalisée implique une série d'étapes telles que la spécification des détails de la structure, la définition d'ensembles de contrôles et la révision de la structure avant de finaliser sa création. Tout au long de ce processus, vous pouvez intégrer les ensembles de contrôle spécifiques à votre organisation, en veillant à ce que le cadre personnalisé reflète fidèlement vos exigences en matière de GRC.

Ressources supplémentaires

Pour obtenir des instructions sur la création d'un framework personnalisé, consultez les ressources suivantes.

- Création d'un cadre personnalisé à partir de zéro dans AWS Audit Manager
- Création d'une copie modifiable d'un framework existant dans AWS Audit Manager

Création d'un cadre personnalisé à partir de zéro dans AWS Audit Manager

Lorsque les exigences de conformité de votre organisation ne correspondent pas aux cadres standard prédéfinis disponibles dans AWS Audit Manager, vous pouvez créer votre propre cadre personnalisé à partir de zéro.

Cette page décrit les étapes à suivre pour créer un cadre personnalisé adapté à vos besoins spécifiques.

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour créer un framework personnalisé dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Tâches

- Étape 1 : Spécifier les détails du framework
- Étape 2 : Spécifier les ensembles de contrôle
- Étape 3 : Examen et création du framework

Étape 1 : Spécifier les détails du framework

Commencez par spécifier les détails de votre framework personnalisé.

Pour spécifier les détails du framework

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Framework library, puis Create custom framework.
3. Dans Détails du framework, entrez un nom, un type de conformité (facultatif) et une description de votre framework (également facultatif). La saisie d'un type de conformité tel que PCI_DSS ou GDPR signifie que vous pouvez utiliser ce mot clé pour rechercher votre framework ultérieurement.
4. Sous Balises, choisissez Ajouter une nouvelle balise pour associer une balise à votre framework. Vous pouvez indiquer une clé et une valeur pour chaque balise. La clé de balise est obligatoire.

Vous pouvez l'utiliser comme critère de recherche lorsque vous recherchez ce framework dans la bibliothèque du framework.

5. Choisissez Suivant.

Étape 2 : Spécifier les ensembles de contrôle

Ensuite, vous spécifiez les contrôles que vous souhaitez ajouter à votre framework et la manière dont vous souhaitez les organiser. Commencez par ajouter des ensembles de contrôles au framework, puis ajoutez des contrôles à l'ensemble de contrôles.

> **Note**
>
> Lorsque vous utilisez la AWS Audit Manager console pour créer une structure personnalisée, vous pouvez ajouter jusqu'à 10 ensembles de contrôles pour chaque structure.
> Lorsque vous utilisez l'API Audit Manager pour créer un framework personnalisé, vous pouvez créer plus de 10 ensembles de contrôles. Pour ajouter plus d'ensembles de contrôles que ce que la console autorise actuellement, utilisez l'CreateAssessmentFrameworkAPI fournie par Audit Manager.

Pour spécifier un ensemble de commandes

1. Sous Nom de l'ensemble de contrôles, entrez un nom pour votre ensemble de contrôles.
2. Sous Ajouter des contrôles, utilisez la liste déroulante des types de contrôle pour sélectionner l'un des deux types de contrôle : contrôles standard ou contrôles personnalisés.
3. En fonction de l'option que vous avez sélectionnée à l'étape précédente, une liste de contrôles standard ou personnalisés s'affiche. Sélectionnez un ou plusieurs contrôles, puis choisissez Ajouter au jeu de contrôles.
4. Dans la fenêtre contextuelle qui apparaît, choisissez Ajouter au jeu de contrôles.
5. Passez en revue les contrôles qui apparaissent dans la liste des contrôles sélectionnés.
   - Pour ajouter d'autres contrôles, répétez les étapes 2 à 4.
   - Pour supprimer les contrôles indésirables, sélectionnez un ou plusieurs contrôles, puis choisissez Supprimer le contrôle.
6. Pour ajouter un nouveau jeu de contrôles, choisissez Ajouter un jeu de contrôles.
7. Pour supprimer un jeu de commandes non désiré, choisissez Supprimer le jeu de contrôles.

8. Une fois que vous avez terminé l'ajout des ensembles de contrôles et des contrôles, choisissez Suivant.

Étape 3 : Examen et création du framework

Vérifiez les informations de votre framework. Pour modifier les informations d'une étape, choisissez Modifier.

Lorsque vous avez terminé, choisissez Créer un framework personnalisé.

Étapes suivantes

Après avoir créé votre nouveau framework personnalisé, vous pouvez créer une évaluation à partir de celui-ci. Pour plus d'informations, consultez Création d'une évaluation dans AWS Audit Manager.

Pour revoir votre framework personnalisé ultérieurement, consultezTrouver les frameworks disponibles dans AWS Audit Manager. Vous pouvez suivre ces étapes pour localiser votre framework personnalisé afin de pouvoir ensuite le visualiser, le modifier, le partager ou le supprimer.

Ressources supplémentaires

Pour des solutions aux problèmes de framework dans Audit Manager, voirRésolution des problèmes liés au framework.

Création d'une copie modifiable d'un framework existant dans AWS Audit Manager

Au lieu de créer une structure personnalisée à partir de zéro, vous pouvez utiliser une structure existante comme point de départ et en créer une copie modifiable. Dans ce cas, le framework existant reste dans la bibliothèque de frameworks, et un nouveau framework personnalisé est créé avec vos paramètres spécifiques.

Vous pouvez créer une copie modifiable de n'importe quel framework existant. Il peut s'agir d'un framework standard ou d'un framework personnalisé.

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour créer un framework personnalisé dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces

autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Tâches

- Étape 1 : Spécifier les détails du framework
- Étape 2 : Spécifier les ensembles de contrôle
- Étape 3 : Examen et création du framework

Étape 1 : Spécifier les détails du framework

Tous les détails du framework, à l'exception des balises, sont repris du framework d'origine. Vérifiez et modifiez ces détails si nécessaire.

Pour spécifier les détails du framework

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Bibliothèque de frameworks.
3. Choisissez le cadre que vous souhaitez utiliser comme point de départ, choisissez Créer un cadre personnalisé, puis sélectionnez Créer une copie.
4. Dans la fenêtre contextuelle qui apparaît, entrez le nom du nouveau cadre personnalisé et choisissez Continuer.
5. Sous Détails du framework, passez en revue le nom, le type de conformité et la description de votre framework, et modifiez-les si nécessaire. Le type de conformité doit indiquer la norme de conformité ou la réglementation associée à votre framework. Vous pouvez utiliser ce mot clé pour rechercher votre framework.
6. Sous Balises, choisissez Ajouter une nouvelle balise pour associer une balise à votre framework. Vous pouvez indiquer une clé et une valeur pour chaque balise. La clé de balise est obligatoire et peut être utilisée comme critère de recherche lorsque vous recherchez ce framework dans la bibliothèque du framework.
7. Choisissez Suivant.

Étape 2 : Spécifier les ensembles de contrôle

Les ensembles de contrôles sont reportés à partir du framework d'origine. Modifiez la configuration actuelle en ajoutant d'autres contrôles ou en supprimant des contrôles existants selon les besoins.

> **Note**
>
> Lorsque vous utilisez la console Audit Manager pour créer un framework personnalisé, vous pouvez ajouter jusqu'à 10 ensembles de contrôles pour chaque framework. Lorsque vous utilisez l'API Audit Manager pour créer un framework personnalisé, vous pouvez ajouter plus de 10 ensembles de contrôles. Pour ajouter plus d'ensembles de contrôles que ce que la console autorise actuellement, utilisez l'CreateAssessmentFrameworkAPI fournie par Audit Manager.

Pour spécifier un ensemble de commandes

1. Sous Nom du jeu de contrôles, modifiez le nom du jeu de contrôles selon vos besoins.
2. Sous Ajouter des contrôles, ajoutez un nouveau contrôle en utilisant la liste déroulante pour sélectionner l'un des deux types de contrôle : contrôles standard ou contrôles personnalisés.
3. En fonction de l'option que vous avez sélectionnée à l'étape précédente, une liste de contrôles standard ou personnalisés s'affiche. Sélectionnez un ou plusieurs contrôles, puis choisissez Ajouter au jeu de contrôles.
4. Dans la fenêtre contextuelle qui apparaît, choisissez Ajouter au jeu de contrôles.
5. Passez en revue les contrôles qui apparaissent dans la liste des contrôles sélectionnés.
   - Pour ajouter d'autres contrôles, répétez les étapes 2 à 4.
   - Pour supprimer les contrôles indésirables, sélectionnez un ou plusieurs contrôles, puis choisissez Supprimer le contrôle.
6. Pour ajouter un nouveau jeu de contrôles à la structure, choisissez Ajouter un jeu de contrôles.
7. Pour supprimer un jeu de commandes non désiré, choisissez Supprimer le jeu de contrôles.
8. Une fois que vous avez terminé l'ajout des ensembles de contrôles et des contrôles, choisissez Suivant.

Étape 3 : Examen et création du framework

Vérifiez les informations de votre framework. Pour modifier les informations d'une étape, choisissez Modifier.

Lorsque vous avez terminé, choisissez Créer un framework personnalisé.

Étapes suivantes

Après avoir créé votre nouveau framework personnalisé, vous pouvez créer une évaluation à partir de celui-ci. Pour plus d'informations, consultez Création d'une évaluation dans AWS Audit Manager.

Pour revoir votre framework personnalisé ultérieurement, consultezTrouver les frameworks disponibles dans AWS Audit Manager. Vous pouvez suivre ces étapes pour localiser votre framework personnalisé afin de pouvoir ensuite le visualiser, le modifier, le partager ou le supprimer.

Ressources supplémentaires

Pour des solutions aux problèmes de framework dans Audit Manager, voirRésolution des problèmes liés au framework.

Modification d'un framework personnalisé dans AWS Audit Manager

Vous devrez peut-être modifier vos frameworks personnalisés au AWS Audit Manager fur et à mesure de l'évolution de vos exigences de conformité.

Cette page décrit les étapes à suivre pour modifier les détails et les ensembles de contrôles d'un framework personnalisé.

Prérequis

La procédure suivante suppose que vous avez déjà créé un framework personnalisé.

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour modifier un framework personnalisé dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Tâches

- Étape 1 : Modifier les détails du framework
- Étape 2 : Modifier les ensembles de contrôles
- Étape 3. Vérifiez et enregistrez

Étape 1 : Modifier les détails du framework

Commencez par examiner et modifier les détails du framework existant.

Modifier les détails du framework

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Bibliothèque de frameworks, puis l'onglet Frameworks personnalisés.
3. Sélectionnez le framework que vous souhaitez modifier, choisissez Actions, puis Modifier.
   - Vous pouvez également ouvrir un cadre personnalisé et choisir Modifier en haut à droite de la page de détails du cadre.
4. Sous Détails du framework, passez en revue le nom, le type de conformité et la description de votre framework, puis apportez les modifications nécessaires.
5. Choisissez Suivant.

> **Tip**
>
> Pour modifier les balises d'un framework, ouvrez le framework et choisissez l'onglet Balises du framework. Vous pouvez y afficher et modifier les balises associées au framework.

Étape 2 : Modifier les ensembles de contrôles

Passez ensuite en revue et modifiez les contrôles et les ensembles de contrôles du framework.

> **Note**
>
> Lorsque vous utilisez la AWS Audit Manager console pour modifier une structure personnalisée, vous pouvez ajouter jusqu'à 10 ensembles de contrôles pour chaque structure.
> Lorsque vous utilisez l'API Audit Manager pour modifier un framework personnalisé, vous pouvez ajouter plus de 10 ensembles de contrôles. Pour ajouter plus d'ensembles de contrôles que ce que la console autorise actuellement, utilisez l'UpdateAssessmentFrameworkAPI fournie par Audit Manager.

Pour modifier un ensemble de contrôles

1. Sous Nom de l'ensemble de contrôles, vérifiez et modifiez le nom de votre ensemble de contrôles selon vos besoins.
2. Sous Ajouter des contrôles, utilisez la liste déroulante des types de contrôle pour sélectionner l'un des deux types de contrôle : contrôles standard ou contrôles personnalisés.
3. En fonction de l'option que vous avez sélectionnée à l'étape précédente, une liste de contrôles standard ou personnalisés s'affiche dans un tableau. Sélectionnez un ou plusieurs contrôles, puis choisissez Ajouter au jeu de contrôles.
4. Dans la fenêtre contextuelle qui apparaît, choisissez Ajouter.
5. Passez en revue et modifiez les contrôles qui apparaissent dans la liste des contrôles sélectionnés.

   - Pour ajouter d'autres contrôles, répétez les étapes 2 à 4.
   - Pour supprimer les contrôles indésirables, sélectionnez un ou plusieurs contrôles, puis choisissez Supprimer du jeu de contrôles.
6. Pour ajouter un nouveau jeu de contrôles à la structure, choisissez Ajouter un jeu de contrôles.
7. Pour supprimer un jeu de commandes non désiré, choisissez Supprimer le jeu de contrôles.
8. Une fois que vous avez terminé l'ajout des ensembles de contrôles et des contrôles, choisissez Suivant.

Étape 3. Vérifiez et enregistrez

Vérifiez les informations de votre framework. Pour modifier les informations d'une étape, choisissez Modifier.

Lorsque vous avez terminé, sélectionnez Enregistrer les modifications.

Étapes suivantes

Lorsque vous êtes certain de ne plus avoir besoin d'un framework personnalisé, vous pouvez nettoyer votre environnement Audit Manager en supprimant le framework. Pour obtenir des instructions, veuillez consulter Suppression d'un framework personnalisé dans AWS Audit Manager.

Ressources supplémentaires

Pour des solutions aux problèmes de framework dans Audit Manager, voirRésolution des problèmes liés au framework.

Partage d'un framework personnalisé dans AWS Audit Manager

Vous pouvez utiliser la fonctionnalité de partage de frameworks AWS Audit Manager pour répliquer rapidement les frameworks personnalisés que vous créez. Vous pouvez partager vos frameworks personnalisés avec un autre Compte AWS, ou les répliquer dans un autre pour Région AWS votre propre compte. Le destinataire peut ensuite accéder à votre framework personnalisé et l'utiliser pour créer des évaluations. Il peut le faire sans avoir à répéter vos efforts de configuration pour ce framework.

Points clés

Pour partager un framework personnalisé, vous devez créer une demande de partage. Le destinataire de la demande de partage dispose alors de 120 jours pour accepter ou refuser la demande. Lorsqu'il accepte la demande de partage, Audit Manager réplique le framework personnalisé partagé dans sa bibliothèque de frameworks. Outre la réplication du framework personnalisé, Audit Manager reproduit également tous les ensembles de contrôles personnalisés et les contrôles personnalisés faisant partie de ce framework. Ces contrôles personnalisés sont ajoutés à la bibliothèque de contrôles du destinataire. Audit Manager ne réplique pas les frameworks ou les contrôles standard. Par défaut, ils sont disponibles dans tous les Comptes AWS et régions où Audit Manager est activé.

La fonctionnalité de partage de framework est disponible uniquement dans la version payante. Cependant, le partage d'un framework personnalisé et l'acceptation d'une demande de partage ne sont soumis à aucuns frais supplémentaires. Pour en savoir plus sur la tarification AWS Audit Manager, consultez la page de AWS Audit Manager tarification.

> **Important**
>
> Vous ne pouvez pas partager un framework personnalisé dérivé d'un framework standard si celui-ci est désigné comme non éligible au partage par AWS, sauf si vous avez obtenu l'autorisation de le faire auprès du propriétaire du framework standard. Pour savoir quels frameworks standard ne sont pas éligibles au partage et en savoir plus, consultez la section Éligibilité au partage des frameworks.

Ressources supplémentaires

Pour en savoir plus sur le partage de frameworks personnalisés dans Audit Manager, consultez les ressources suivantes.

- Concepts et terminologie de partage de frameworks
- Envoi d'une demande pour partager un framework personnalisé dans AWS Audit Manager
- Répondre aux demandes de partage dans AWS Audit Manager
- Supprimer des demandes de partage dans AWS Audit Manager

Concepts et terminologie de partage de frameworks

Si vous découvrez les concepts clés suivants, vous pourrez tirer le meilleur parti de la fonctionnalité de partage de frameworks personnalisés AWS Audit Manager .

Points clés

Expéditeur

Il s'agit du créateur d'une demande de partage et de l' Compte AWS endroit où le framework personnalisé existe. Les expéditeurs peuvent partager des frameworks personnalisés avec n'importe Compte AWS qui. Ou bien, ils répliquent un framework personnalisé sur n'importe quel framework pris en Région AWS charge pour leur propre compte.

Destinataire

C'est le consommateur du framework partagé. Les destinataires peuvent accepter ou refuser une demande de partage émanant d'un expéditeur.

> **Note**
>
> Un destinataire peut être un compte administrateur délégué. Toutefois, vous ne pouvez pas partager de frameworks personnalisés avec un compte AWS Organizations de gestion.

Éligibilité du framework

Vous pouvez uniquement partager des frameworks personnalisés. Par défaut, les frameworks standard sont déjà présents dans tous les environnements Comptes AWS et Régions AWS là où AWS Audit Manager c'est activé. En outre, les frameworks personnalisés que vous partagez ne doivent pas contenir de données sensibles. Cela inclut les données présentes dans le framework lui-même, ses ensembles de contrôles et tous les contrôles personnalisés inclus dans le framework personnalisé.

> **Important**
>
> Certains des frameworks standard proposés par AWS Audit Manager contiennent du matériel protégé par des droits d'auteur soumis à des contrats de licence. Les frameworks personnalisés peuvent contenir du contenu dérivé de ces frameworks. Vous ne pouvez pas partager un framework personnalisé dérivé d'un framework standard si celui-ci est désigné comme non éligible au partage par AWS, sauf si vous avez obtenu l'autorisation de le faire auprès du propriétaire du framework standard.
> Pour savoir quels frameworks standard sont éligibles au partage, reportez-vous au tableau suivant.

Nom du framework standard	Versions personnalisées éligibles au partage
Centre australien de cybersécurité (ACSC) Essential Eight	 Oui

Nom du framework standard	Versions personnalisées éligibles au partage
Manuel de sécurité de l'information (ISM) du Centre australien de cybersécurité (ACSC) 02 mars 2023	 Oui
Exemple de framework d'Audit Manager pour Amazon Web Services (AWS)	 Oui
Barrières de protection AWS Control Tower	 Oui
AWS Cadre des meilleures pratiques d'IA générative v2	 Oui
Gestionnaire de licences AWS	 Oui
AWS Bonnes pratiques de sécurité fondamentales	 Oui
AWS Bonnes pratiques opérationnelles	 Oui
Amazon Web Services (AWS) Well Architected Framework (WAF) v10	 Oui

Nom du framework standard	Versions personnalisées éligibles au partage
Centre canadien pour la cybersécurité (CCCS) pour le contrôle moyen du cloud	Non
Centre de sécurité Internet (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, niveau 1	Non
Centre de sécurité Internet (CIS) Amazon Web Services (AWS) Benchmark v1.2.0, niveaux 1 et 2	Non
Centre de sécurité Internet (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, niveau 1	Non
Centre de sécurité Internet (CIS) Amazon Web Services (AWS) Benchmark v1.3.0, niveaux 1 et 2	Non
Centre de sécurité Internet (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, niveau 1	Non
Centre de sécurité Internet (CIS) Amazon Web Services (AWS) Benchmark v1.4.0, niveaux 1 et 2	Non
Centre pour la sécurité Internet (CIS) v7.1, IG1	Oui

Nom du framework standard	Versions personnalisées éligibles au partage
Contrôles de sécurité critiques CIS version 8.0 (CIS v8.0), IG1	Non
Contrôles de base de sécurité du Programme fédéral de gestion des risques et des autorisations (FedRAMP) r4, modérés	Oui
Règlement général sur la protection des données (RGPD) 2016	Oui
Loi Gramm-Leach-Bliley (GLBA)	Oui
Titre 21 du Code des règlements fédéraux (CFR), partie 11, Enregistrements électroniques ; signatures électroniques - Champ d'application et application 24 mai 2023	Oui
EudraLex - Les règles régissant les médicaments dans l'Union européenne (UE) - Volume 4 : Bonnes pratiques de fabrication (GMP) pour les médicaments à usage humain et vétérinaire - Annexe 11	Oui
Règle de sécurité de la Health Insurance Portability and Accountability Act (HIPAA) : février 2003	Oui
Règle finale omnibus de la Health Insurance Portability and Accountability Act (HIPAA)	Oui

Nom du framework standard	Versions personnalisées éligibles au partage
Organisation internationale de normalisation (ISO) /Commission électrotechnique internationale (CEI) 27001:2013 Annexe A	Non
NIST 800-53 Rev 5 : Contrôles de sécurité et de confidentialité pour les systèmes d'information et les organisations	Oui
Cadre de cybersécurité du NIST (CSF) v1.1	Oui
NIST 800-171 Revision 2 : Protection des informations contrôlées non classifiées dans les systèmes et organisations non fédéraux	Oui
Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) v3.2.1	Non
Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) v4.0	Non
Déclaration sur les normes pour l'engagement des attestations (SSAE) n° 18, rapport 2 du Service Organizations Controls (SOC)	Non

Demande de partage

Pour partager un framework personnalisé, vous devez créer une demande de partage. La demande de partage indique un destinataire et l'informe qu'un framework personnalisé est disponible. Les destinataires ont 120 jours pour répondre à une demande de partage en l'acceptant ou en la refusant. Si aucune action n'est entreprise dans les 120 jours, la demande

de partage expire et le destinataire perd la possibilité d'ajouter le framework personnalisé à sa bibliothèque de frameworks. Les expéditeurs et les destinataires peuvent consulter les demandes de partage et y donner suite depuis la page des demandes de partage de la bibliothèque de frameworks.

Statut des demandes de partage

Les demandes de partage peuvent présenter les statuts suivants.

État	Description
Actif	Cela indique qu'une demande de partage a été envoyée avec succès au destinataire et attend une réponse de ce dernier.
Expirant	Cela indique une demande de partage qui expirera dans les 30 prochains jours.
Partagé	Cela indique une demande de partage acceptée par le destinataire.
Inactif	Cela indique qu'une demande de partage a été révoquée, refusée ou a expiré avant que le destinataire n'agisse.
Réplication	Cela indique une demande de partage acceptée qui est répliquée dans la bibliothèque de cadres du destinataire.
Échec	Cela indique qu'une demande de partage n'a pas été envoyée avec succès au destinataire.

Notifications de demande de partage

Audit Manager informe les destinataires lorsqu'ils reçoivent une demande de partage. Les destinataires et les expéditeurs reçoivent une notification lorsqu'une demande de partage expire dans les 30 prochains jours.

- Pour les destinataires, un point de notification bleu apparaît à côté des demandes reçues ayant le statut Actif ou Arrive à expiration. Le destinataire peut agir sur la notification en acceptant ou en refusant la demande de partage.
- Pour les destinataires, un point de notification bleu apparaît à côté des demandes reçues ayant le statut Arrive à expiration. La notification est classée lorsque le destinataire accepte ou refuse

la demande de partage. Dans le cas contraire, elle est classée à l'expiration de la demande. En outre, l'expéditeur peut agir sur la notification en révoquant la demande de partage.

Propriété de l'expéditeur

Les expéditeurs conservent un accès complet aux frameworks personnalisés qu'ils partagent. Ils peuvent annuler les demandes de partage actives à tout moment en révoquant la demande de partage avant son expiration. Toutefois, une fois qu'un destinataire a accepté une demande de partage, l'expéditeur ne peut plus révoquer l'accès du destinataire à ce framework personnalisé. En effet, lorsque le destinataire accepte la demande, Audit Manager crée une copie indépendante du framework personnalisé dans la bibliothèque de frameworks du destinataire.

Outre la réplication du framework personnalisé de l'expéditeur, Audit Manager reproduit également tous les ensembles de contrôles personnalisés et les contrôles personnalisés faisant partie de ce framework. Toutefois, Audit Manager ne réplique aucune balise attachée au framework personnalisé.

Propriété du destinataire

Les destinataires ont un accès complet aux frameworks personnalisés qu'ils acceptent. Lorsque le destinataire accepte la demande, Audit Manager réplique le framework personnalisé dans l'onglet Frameworks personnalisés de sa bibliothèque de frameworks. Les destinataires peuvent ensuite gérer le framework personnalisé partagé de la même manière que n'importe quel autre framework personnalisé. Les destinataires peuvent partager les frameworks personnalisés qu'ils reçoivent d'autres expéditeurs. Les destinataires ne peuvent empêcher les expéditeurs d'envoyer des demandes de partage.

Expiration du framework partagé

Lorsqu'un expéditeur crée une demande de partage, Audit Manager configure la demande pour qu'elle expire au bout de 120 jours. Les destinataires peuvent accepter le framework partagé et y accéder avant l'expiration de la demande. Si un destinataire ne l'accepte pas pendant cette période, la demande de partage expire. À partir de là, un enregistrement de la demande de partage expirée reste dans son historique. Les instantanés des frameworks partagés expirés sont archivés dans un compartiment S3 avec un TTL d'un an à des fins d'audit.

Les expéditeurs peuvent choisir de révoquer une demande de partage à tout moment avant son expiration.

Sauvegarde et stockage des données du framework partagé

Lorsque vous créez une demande de partage, Audit Manager stocke un instantané de votre framework personnalisé dans l'est des États-Unis (Virginie du Nord) Région AWS. Audit Manager stocke également une sauvegarde du même instantané dans l'ouest des États-Unis (Oregon) Région AWS.

Audit Manager supprime l'instantané et l'instantané de sauvegarde lorsque l'un des événements suivants se produit :

- L'expéditeur révoque la demande de partage.
- Le destinataire refuse la demande de partage.
- Le destinataire rencontre une erreur et n'accepte pas correctement la demande de partage.
- La demande de partage expire avant que le destinataire ne réponde à la demande.

Lorsqu'un expéditeur renvoie une demande de partage, l'instantané est remplacé par une version mise à jour correspondant à la dernière version du framework personnalisé.

Lorsqu'un destinataire accepte une demande de partage, le cliché est répliqué dans le fichier Compte AWS sous la Région AWS forme spécifiée dans la demande de partage.

Gestion des versions des frameworks partagés

Lorsque vous partagez un framework personnalisé, Audit Manager crée une copie indépendante de ce framework dans la région spécifiée Compte AWS . Cela signifie que vous devez garder à l'esprit les points suivants :

- Le framework partagé qu'un destinataire accepte est un instantané du framework au moment de la création de la demande de partage. Si vous mettez à jour le framework personnalisé d'origine après avoir envoyé une demande de partage, celle-ci n'est pas automatiquement mise à jour. Pour partager la dernière version du framework mis à jour, vous pouvez renvoyer la demande de partage. La date d'expiration de ce nouvel instantané est de 120 jours à compter de la date du nouveau partage.
- Lorsque vous partagez un cadre personnalisé avec un autre, Compte AWS puis que vous le supprimez de votre bibliothèque de cadres, le cadre personnalisé partagé reste dans la bibliothèque de cadres du destinataire.
- Lorsque vous partagez un cadre personnalisé avec un autre Région AWS utilisateur de votre compte, puis que vous supprimez ce cadre personnalisé dans le premier Région AWS, le cadre personnalisé reste dans la deuxième région.

- Lorsque vous supprimez un framework personnalisé partagé après l'avoir accepté, tous les contrôles personnalisés répliqués dans le cadre du framework personnalisé restent dans votre bibliothèque de contrôles.

Ressources supplémentaires

- Envoi d'une demande pour partager un framework personnalisé dans AWS Audit Manager
- Répondre aux demandes de partage dans AWS Audit Manager
- Supprimer des demandes de partage dans AWS Audit Manager
- Résolution des problèmes liés au framework

Envoi d'une demande pour partager un framework personnalisé dans AWS Audit Manager

Ce didacticiel explique comment partager vos frameworks personnalisés entre Comptes AWS et Régions AWS.

Lorsque vous partagez un framework personnalisé, Audit Manager crée un instantané de votre framework et envoie une demande de partage au destinataire. Le destinataire dispose de 120 jours pour accepter le framework partagé. Lorsqu'il accepte la demande de partage, Audit Manager réplique le framework personnalisé partagé dans sa bibliothèque de frameworks dans la Région AWS spécifiée. Si vous souhaitez répliquer un framework personnalisé dans une autre région sous votre propre compte, utilisez le didacticiel suivant et entrez votre propre Compte AWS identifiant comme identifiant de compte du destinataire.

Prérequis

Avant de commencer ce tutoriel, vérifiez d'abord que vous remplissez les conditions suivantes :

- Vous connaissez les concepts et la terminologie de partage de frameworks Audit Manager.
- Le framework personnalisé que vous souhaitez partager est éligible au partage et existe dans la bibliothèque de frameworks de votre environnement AWS Audit Manager .
- Le destinataire a déjà activé AWS Audit Manager l' Région AWS endroit où vous souhaitez partager le framework personnalisé.
- Le destinataire n'est pas un compte AWS Organizations de gestion.

- Votre identité IAM dispose des autorisations appropriées pour partager un framework personnalisé. AWS Audit Manager Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

> **Tip**
>
> Avant de commencer, notez l' Compte AWS identifiant avec lequel vous souhaitez partager votre framework personnalisé. Il peut s'agir de votre propre identifiant de compte, si votre objectif est de reproduire le framework sur un autre Région AWS sous votre compte. Vous aurez besoin de ces informations à l'étape 2 de ce tutoriel.

Procédure

Tâches

- Étape 1 : Identifier le framework personnalisé que vous souhaitez partager
- Étape 2 : Envoyer une demande de partage
- Étape 3 : Afficher vos demandes envoyées
- Étape 4 (Facultatif) : Révoquer la demande de partage

Étape 1 : Identifier le framework personnalisé que vous souhaitez partager

Commencez par identifier le framework personnalisé que vous souhaitez partager. Vous pouvez consulter tous les frameworks personnalisés disponibles sur la page Bibliothèque de frameworks d'Audit Manager.

> **Important**
>
> Ne partagez pas de frameworks personnalisés contenant des données sensibles. Cela inclut les données présentes dans le framework lui-même, ses ensembles de contrôles et tous les contrôles personnalisés qui composent le framework personnalisé. Pour plus d'informations, consultez Éligibilité du framework.

Pour consulter vos frameworks personnalisés disponibles

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Bibliothèque de frameworks.
3. Choisissez l'onglet Frameworks personnalisés. Cela affiche une liste de vos frameworks personnalisés disponibles. Vous pouvez choisir un nom de framework pour afficher les détails de ce framework personnalisé.

Étape 2 : Envoyer une demande de partage

Ensuite, spécifiez un destinataire et envoyez-lui une demande de partage pour le framework personnalisé. La destinataire dispose de 120 jours pour répondre à cette demande de partage avant qu'elle n'expire.

Pour envoyer une demande de partage

1. Dans l'onglet Frameworks personnalisés de la bibliothèque de frameworks, choisissez le nom d'un framework pour ouvrir la page de détails. À partir de là, choisissez Actions, puis sélectionnez Partager le framework personnalisé.
   - Vous pouvez également sélectionner un framework personnalisé dans la liste de la bibliothèque de frameworks, choisir Actions, puis Partager le framework personnalisé. En fonction de la taille du framework personnalisé, cette méthode peut prendre quelques secondes, le temps qu'Audit Manager prépare la demande de partage.
2. Consultez l'avis qui s'affiche dans la boîte de dialogue.
   - Si vous ne savez pas si vous pouvez partager votre framework personnalisé, consultez Éligibilité du framework pour obtenir des conseils supplémentaires.
   - Si votre infrastructure comporte des contrôles qui utilisent des AWS Config règles personnalisées comme source de données, nous vous recommandons de contacter le destinataire pour le lui faire savoir. Le destinataire peut ensuite créer et activer les mêmes AWS Config règles dans son instance de AWS Config. Pour plus d'informations, consultez Mon framework partagé comporte des contrôles qui utilisent des AWS Config règles personnalisées comme source de données. Le destinataire peut-il collecter des éléments probants pour ces contrôles ?.
3. Saisissez **`agree`**, puis choisissez Accepter pour continuer.
4. Sur l'écran suivant, procédez comme suit :

- Dans Compte AWS, saisissez l'identifiant de compte du destinataire. Il peut s'agir de votre propre ID de compte.
- Dans Région AWS, sélectionnez la région du destinataire dans la liste déroulante.
- (Facultatif) Sous Message au destinataire, entrez un commentaire facultatif concernant le framework personnalisé que vous partagez.
- Sous Détails du framework personnalisé, passez en revue les détails pour confirmer que vous souhaitez partager ce framework.

5. Choisissez Partager.

> **Note**
>
> Gardez les points suivants à l'esprit :
>
> - Lorsque vous partagez un framework personnalisé avec un autre Compte AWS, le framework est répliqué uniquement vers le framework spécifié Région AWS. Après avoir accepté la demande de partage, le destinataire peut ensuite reproduire le framework dans toutes les régions selon ses besoins.
> - Lorsque vous partagez des frameworks personnalisés entre Régions AWS eux, le traitement des actions de demande de partage peut prendre jusqu'à 10 minutes. Après avoir envoyé une demande de partage entre régions, nous vous recommandons de revenir ultérieurement vérifier que votre demande de partage a bien été envoyée.
> - Lorsque vous envoyez une demande de partage, Audit Manager prend un instantané du framework personnalisé au moment de la création de la demande de partage. Si vous mettez à jour le framework personnalisé d'origine après avoir envoyé une demande de partage, la demande n'est pas automatiquement mise à jour. Pour partager la dernière version d'un framework mis à jour, vous pouvez renvoyer la demande de partage. La date d'expiration de ce nouvel instantané est de 120 jours à compter de la date du nouveau partage.

Étape 3 : Afficher vos demandes envoyées

Vous pouvez sélectionner l'onglet Demandes envoyées pour afficher la liste de toutes les demandes de partage que vous avez envoyées. Vous pouvez filtrer cette liste selon vos besoins. Par exemple,

vous pouvez appliquer des filtres pour afficher uniquement les demandes qui expirent dans les 30 prochains jours.

Pour consulter et filtrer les demandes que vous avez envoyées

1. Dans le panneau de navigation, sélectionnez Demandes de partage.
2. Choisissez l'onglet Demandes envoyées.
3. (Facultatif) Appliquez des filtres pour affiner les demandes envoyées qui sont visibles. Pour ce faire, recherchez la liste déroulante Tous les statuts et remplacez le filtre par l'un des filtres suivants.

État	Description
Actif	Ce filtre affiche les demandes de partage en attente d'une réponse du destinataire.
Expirant	Ce filtre affiche les demandes de partage qui expirent dans les 30 prochains jours.
Partagé	Ce filtre affiche les demandes de partage acceptées par le destinataire. Le framework personnalisé partagé existe désormais dans la bibliothèque de frameworks du destinataire.
Inactif	Ce filtre affiche les demandes de partage qui ont été refusées, révoquées ou expirées avant que le destinataire n'intervienne. Choisissez le mot Inactif pour afficher plus de détails.
Réplication	Cela indique une demande de partage acceptée qui est répliquée dans la bibliothèque de cadres du destinataire.
Échec	Ce filtre affiche les demandes de partage qui n'ont pas été envoyées avec succès au destinataire. Choisissez le mot Échec pour afficher plus de détails.

> **Note**
>
> Le traitement d'une demande de partage peut prendre jusqu'à 15 minutes. Par conséquent, si une erreur se produit lors de l'envoi de votre demande de partage au destinataire, le statut

Échec risque de ne pas s'afficher immédiatement. Nous vous recommandons de revenir ultérieurement vérifier que votre demande de partage a bien été envoyée.

Étape 4 (Facultatif) : Révoquer la demande de partage

Si vous devez annuler une demande de partage active avant son expiration, vous pouvez la révoquer à tout moment. Cette étape est facultative. Si vous ne faites rien, le destinataire ne sera plus en mesure d'accepter la demande de partage après la date d'expiration.

Pour révoquer une demande de partage

1. Dans le panneau de navigation, sélectionnez Demandes de partage.
2. Choisissez l'onglet Demandes envoyées.
3. Sélectionnez le framework que vous souhaitez révoquer, puis Révoquer la demande.
4. Dans la fenêtre contextuelle qui s'affiche, choisissez Révoquer.

> **Note**
>
> Vous ne pouvez révoquer l'accès qu'aux demandes de partage dont le statut est Actif ou Arrive à expiration. Une fois qu'un destinataire a accepté une demande de partage, vous ne pouvez plus révoquer l'accès du destinataire à ce framework personnalisé. Cela est dû au fait qu'une copie du framework personnalisé existe désormais dans la bibliothèque de frameworks du destinataire.
>
> Lorsque vous partagez des frameworks entre Régions AWS eux, le traitement des actions de demande de partage peut prendre jusqu'à 10 minutes. Après avoir révoqué une demande de partage entre régions, nous vous recommandons de revenir ultérieurement vérifier que votre demande de partage a bien été révoquée.

Étapes suivantes

Renvoi d'une demande de partage pour un framework mis à jour

Vous pouvez envoyer une demande de partage pour un framework personnalisé, puis mettre à jour le même framework par la suite. Dans ce cas, la demande de partage n'est pas automatiquement mise à jour pour refléter la dernière version du framework. Toutefois, si le statut est Actif, Partagé ou Arrive

à expiration, vous pouvez mettre à jour une demande de partage existante. Pour ce faire, vous devez renvoyer une nouvelle demande de partage avec les mêmes informations que la demande existante. Dans la nouvelle demande de partage, incluez le même identifiant de framework personnalisé, le même identifiant de compte destinataire et la même Région AWS destinataire. Vous pouvez également ajouter un nouveau commentaire à la nouvelle demande de partage.

Gardez à l'esprit les points suivants lorsque vous renvoyez une demande de partage :

- Pour que la mise à jour soit réussie, la nouvelle demande doit concerner le même identifiant de framework personnalisé. Elle doit également spécifier le même numéro de compte destinataire et la même région que pour la demande existante.
- Si le nom du framework personnalisé a changé, la demande de partage mise à jour affiche le nom le plus récent.
- Si vous fournissez un nouveau commentaire, la demande de partage mise à jour affiche le dernier commentaire.
- Lorsque vous renvoyez une demande de partage, la date d'expiration est prolongée de six mois.

Pour renvoyer une demande de partage pour un framework mis à jour

1. Dans l'onglet Frameworks personnalisés de la bibliothèque de frameworks, choisissez le nom du framework que vous souhaitez partager. Cette action ouvre la page détaillée du framework.
2. Choisissez Actions, puis sélectionnez Partager le cadre personnalisé.
3. Consultez l'avis qui s'affiche dans la boîte de dialogue, entrez **`agree`**, puis choisissez Accepter pour continuer.
4. Sur l'écran suivant, procédez comme suit :
    - Sous Compte AWS, entrez le même identifiant de compte que celui que vous avez spécifié dans la demande de partage existante.
    - Sous Région AWS, entrez la même région que celle que vous avez spécifiée dans la demande de partage existante.
    - (Facultatif) Sous Message au destinataire, entrez un commentaire facultatif concernant le framework personnalisé mis à jour.
    - Sous Détails du framework personnalisé, passez en revue les détails pour confirmer que vous souhaitez renvoyer la demande de partage.
5. Choisissez Partager pour renvoyer et mettre à jour la demande de partage.

Ressources supplémentaires

Pour trouver des solutions aux problèmes que vous pouvez rencontrer lors du partage d'un framework personnalisé, consultezRésolution des problèmes liés au framework.

Répondre aux demandes de partage dans AWS Audit Manager

Ce tutoriel décrit les actions à effectuer lorsque vous recevez une demande de partage pour un framework personnalisé. Audit Manager vous informe lorsque vous recevez une demande de partage. Vous recevez aussi une notification lorsqu'une demande de partage expire dans les 30 prochains jours.

Prérequis

Avant de commencer, nous vous recommandons d'en apprendre plus sur les concepts et la terminologie de partage de framework Audit Manager.

Procédure

Tâches

- Étape 1 : Vérifier les notifications de demande que vous avez reçues
- Étape 2 : Agir sur une demande
- Étape 3 : Afficher l'historique des demandes que vous avez reçues

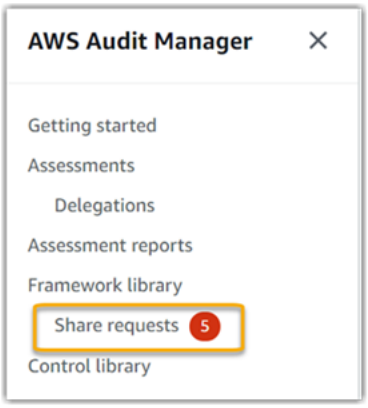
Étape 1 : Vérifier les notifications de demande que vous avez reçues

Commencez par vérifier vos notifications de demande de partage. L'onglet Demandes reçues affiche la liste des demandes de partage que vous avez reçues d'autres personnes Comptes AWS. Les demandes en attente de réponse apparaissent avec un point bleu. Vous pouvez également filtrer cette vue pour n'afficher que les demandes qui expirent dans les 30 prochains jours.

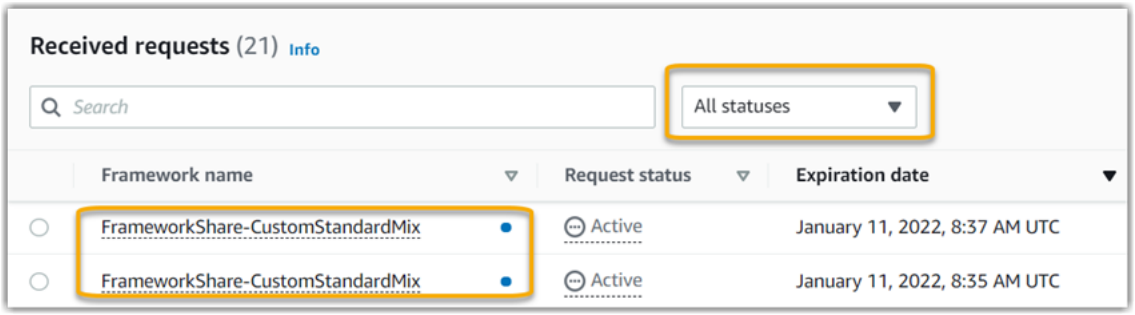
Pour consulter les demandes reçues

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Si vous avez reçu une notification de demande de partage, Audit Manager affiche un point rouge à côté de l'icône du menu de navigation.

3. Développez le volet de navigation et regardez à côté de Demandes de partage. Un badge de notification indique le nombre de demandes de partage qui nécessitent votre attention.



4. Choisissez Demandes de partage. Par défaut, cette page s'ouvre dans l'onglet Demandes reçues.
5. Identifiez les demandes de partage qui nécessitent une action de votre part en recherchant les éléments marqués d'un point bleu.



6. (Facultatif) Pour afficher uniquement les demandes qui expireront dans les 30 prochains jours, recherchez la liste déroulante Tous les statuts et sélectionnez Arrive à expiration.

Étape 2 : Agir sur une demande

Pour supprimer le point de notification bleu, vous devez agir en acceptant ou en refusant la demande de partage.

Accepter un framework partagé

Lorsque vous acceptez une demande de partage, Audit Manager réplique un instantané du framework d'origine dans l'onglet Frameworks personnalisés de votre bibliothèque de frameworks.

Audit Manager réplique et chiffre le nouveau framework personnalisé à l'aide de la clé KMS que vous avez spécifiée dans vos Paramètres Audit Manager.

Pour accepter une demande de partage

1. Ouvrez la page Demandes de partage et assurez-vous de consulter l'onglet Demandes reçues.
2. (Facultatif) Sélectionnez Actif ou Arrive à expiration dans la liste déroulante des filtres.
3. (Facultatif) Choisissez un nom de framework pour afficher les détails de la demande de partage. Cela inclut des informations comme la description du framework, le nombre de contrôles présents dans le framework et le message de l'expéditeur.
4. Sélectionnez la demande de partage que vous souhaitez accepter, choisissez Actions, puis Accepter.

Une fois que vous avez accepté une demande de partage, le statut passe à Réplication, tandis que le framework personnalisé partagé est ajouté à votre bibliothèque de frameworks. Si le framework contient des contrôles personnalisés, ces contrôles sont ajoutés à votre bibliothèque de contrôles pour le moment.

Une fois le framework répliqué, le statut devient Partagé. Une bannière de réussite vous indique que le framework personnalisé est prêt à être utilisé.

> **Tip**
>
> Lorsque vous acceptez un framework personnalisé, il est répliqué uniquement sur dans votre Région AWS actuelle. Vous souhaiterez peut-être que le nouveau framework partagé soit disponible dans toutes les régions de votre Compte AWS. Si tel est le cas, après avoir accepté la demande de partage, vous pouvez partager le framework avec d'autres régions sous votre compte selon vos besoins.

Refuser un partage de framework

Lorsque vous refusez une demande de partage, Audit Manager n'ajoute pas ce framework personnalisé à votre bibliothèque de frameworks. Cependant, un enregistrement de la demande de partage refusée reste dans l'onglet Demandes reçues, avec le statut Inactif.

Pour refuser une demande de partage

1. Ouvrez la page Demandes de partage et assurez-vous de consulter l'onglet Demandes reçues.
2. (Facultatif) Sélectionnez Actif ou Arrive à expiration dans la liste déroulante des filtres.
3. (Facultatif) Choisissez un nom de framework pour afficher les détails de la demande de partage. Cela inclut des informations comme la description du framework, le nombre de contrôles présents dans le framework et le message de l'expéditeur.
4. Sélectionnez la demande de partage que vous souhaitez refuser, choisissez Actions, puis Refuser.
5. Dans la boîte de dialogue qui s'affiche, choisissez Refuser pour confirmer votre choix.

> **Tip**
>
> Si vous changez d'avis et souhaitez accéder à un framework partagé après avoir refusé, demandez à l'expéditeur de vous envoyer une nouvelle demande de partage.

> **Note**
>
> Le traitement des actions de demande de partage peut prendre jusqu'à 10 minutes lors d'un partage de framework entre Régions AWS. Après avoir accepté une demande de partage entre régions, nous vous recommandons de revenir ultérieurement vérifier que votre demande de partage a bien été acceptée ou refusée.

Étape 3 : Afficher l'historique des demandes que vous avez reçues

Après avoir accepté ou refusé un framework partagé, vous pouvez revenir à la page Demandes de partage pour consulter l'historique de vos demandes de partage. Vous pouvez filtrer cette liste selon vos besoins. Par exemple, vous pouvez appliquer des filtres pour afficher uniquement les demandes que vous avez acceptées.

Pour consulter l'historique de vos demandes de partage

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation de gauche, sélectionnez Demandes de partage.
3. Choisissez l'onglet Demandes reçues.

4. Recherchez la liste déroulante Tous les statuts, puis sélectionnez l'un des filtres suivants :

Name (Nom)	Description
Actif	Ce filtre affiche les demandes de partage que vous n'avez pas encore acceptées ou refusées.
Expirant	Ce filtre affiche les demandes de partage qui expirent dans les 30 prochains jours.
Partagé	Ce filtre affiche les demandes de partage que vous avez acceptées. Le framework partagé est désormais disponible dans votre bibliothèque de frameworks.
Inactif	Ce filtre affiche les demandes de partage qui ont été refusées ou ont expiré.
Échec	Ce filtre affiche les demandes de partage qui n'ont pas été envoyées correctement. Choisissez le mot Échec pour afficher plus de détails.

Étapes suivantes

Une fois que vous avez accepté un framework personnalisé partagé, vous pouvez le trouver dans l'onglet Frameworks personnalisés de la bibliothèque du frameworks. Vous pouvez désormais utiliser ce framework pour créer une évaluation. Pour en savoir plus, veuillez consulter la section Création d'une évaluation dans AWS Audit Manager.

Pour obtenir des instructions sur la façon de modifier votre nouveau cadre personnalisé, consultezModification d'un framework personnalisé dans AWS Audit Manager.

Ressources supplémentaires

Pour trouver des solutions aux problèmes que vous pourriez rencontrer, consultezRésolution des problèmes liés au framework.

Supprimer des demandes de partage dans AWS Audit Manager

Lorsque vous n'avez plus besoin d'une demande de partage, vous pouvez la supprimer de votre environnement Audit Manager. Cela vous permet de nettoyer votre espace de travail et de vous concentrer sur les demandes correspondant à vos tâches et priorités actuelles.

Lorsque vous supprimez une demande de partage, seule la demande elle-même est supprimée. Le framework partagé lui-même reste dans votre bibliothèque de frameworks.

Prérequis

La procédure suivante suppose que vous avez déjà envoyé ou reçu une demande de partage. Vous ne pouvez pas supprimer les demandes de partage dont le statut est Actif ou Réplication.

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour supprimer une demande de partage dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Pour supprimer demande de partage

1. Dans le panneau de navigation, sélectionnez Demandes de partage.
2. Choisissez l'onglet Demandes envoyées ou Demandes reçues.
3. Sélectionnez le framework que vous ne souhaitez plus, puis choisissez Supprimer.
4. Dans la fenêtre contextuelle qui s'affiche, choisissez Supprimer.

Ressources supplémentaires

Pour trouver des solutions aux problèmes que vous pourriez rencontrer, consultezRésolution des problèmes liés au framework.

Suppression d'un framework personnalisé dans AWS Audit Manager

Lorsque vous n'avez plus besoin d'un framework personnalisé, vous pouvez le supprimer de votre environnement Audit Manager. Cela vous permet de nettoyer votre espace de travail et de vous concentrer sur les cadres personnalisés adaptés à vos tâches et priorités actuelles.

Prérequis

La procédure suivante suppose que vous avez déjà créé un framework personnalisé.

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour supprimer un framework personnalisé dans AWS Audit Manager. Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Vous pouvez supprimer des frameworks personnalisés à l'aide de la console Audit Manager, de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

> **Note**
>
> La suppression d'un framework personnalisé n'affecte pas les évaluations existantes créées à partir du framework avant sa suppression.

Audit Manager console

Pour supprimer un framework personnalisé sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Bibliothèque de frameworks, puis l'onglet Frameworks personnalisés.
3. Sélectionnez le framework que vous souhaitez supprimer, choisissez Actions, puis Modifier.
   - Vous pouvez également ouvrir un framework personnalisé et choisir Actions, Supprimer en haut à droite de la page de résumé du framework.
4. Dans la fenêtre contextuelle, choisissez Supprimer pour confirmer la suppression.

AWS CLI

Pour supprimer un cadre personnalisé dans AWS CLI

1. Identifiez d'abord le framework personnalisé que vous souhaitez supprimer. Pour ce faire, exécutez la list-assessment-frameworkscommande et spécifiez le `--framework-type` as`Custom`.

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom
   ```

   La réponse renvoie une liste de frameworks personnalisés. Recherchez le framework personnalisé que vous souhaitez supprimer et prenez note de l'ID du framework.

2. Ensuite, exécutez la delete-assessment-frameworkcommande et spécifiez le `--framework-id` framework que vous souhaitez supprimer.

   Dans l'exemple suivant, remplacez le *`texte de l'espace réservé`* par vos propres informations.

   ```
   aws auditmanager delete-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

Pour supprimer un framework personnalisé à l'aide de l'API

1. Utilisez l'ListAssessmentFrameworksopération et spécifiez le FrameworkType comme. `Custom` Pour la réponse, recherchez le framework personnalisé que vous souhaitez supprimer et prenez note de l'ID du framework.
2. Utilisez cette DeleteAssessmentFrameworkopération pour supprimer le cadre. Dans la requête, utilisez le paramètre frameworkId pour spécifier le framework que vous souhaitez supprimer.

Pour plus d'informations sur ces opérations d'API, cliquez sur l'un des liens de la procédure précédente pour en savoir plus dans la référence des AWS Audit Manager API. Cela inclut des informations sur la façon d'utiliser ces opérations et paramètres dans l'un des SDK spécifiques au langage AWS .

Ressources supplémentaires

Pour plus d'informations sur la conservation des données dans Audit Manager, consultezSuppression des données d'Audit Manager.

Utilisation de la bibliothèque de commandes pour gérer les commandes dans AWS Audit Manager

Vous pouvez accéder aux commandes et les gérer à partir de la bibliothèque de commandes située dans AWS Audit Manager.

Points clés

Dans la bibliothèque de commandes, les commandes sont organisées dans les catégories suivantes.

- Les contrôles communs collectent des preuves à l'appui de plusieurs normes de conformité qui se chevauchent. Les contrôles communs automatisés contiennent un ou plusieurs contrôles de base connexes qui collectent chacun des preuves à l'appui à partir d'un groupe prédéfini de sources de données. Cela vous permet d'identifier efficacement les sources de AWS données correspondant à votre portefeuille d'exigences de conformité. Les sources de données sous-jacentes à chaque contrôle commun automatisé sont validées et gérées par des évaluateurs certifiés par le secteur au sein des services d'assurance AWS de sécurité.
- Les contrôles standard collectent des preuves à l'appui d'une norme de conformité spécifique. Vous pouvez consulter les détails des contrôles standard, mais vous ne pouvez ni les modifier ni les supprimer. Cependant, vous pouvez créer une copie modifiable de n'importe quel contrôle standard pour créer un nouveau contrôle répondant à vos besoins spécifiques.
- Les contrôles personnalisés sont des contrôles que vous possédez et que vous définissez. Lorsque vous créez un contrôle personnalisé, nous vous recommandons de choisir les contrôles courants qui représentent vos objectifs et de les utiliser comme source de preuves. Par conséquent, votre contrôle personnalisé peut collecter toutes les preuves pertinentes pour ces contrôles courants. Vous pouvez également utiliser les contrôles de base comme source de preuves ou utiliser d'autres sources que vous définissez vous-même. Lorsque vous avez terminé, ajoutez vos contrôles personnalisés à un cadre personnalisé, puis créez une évaluation pour commencer à recueillir des preuves.

Ressources supplémentaires

Pour créer et gérer des contrôles dans Audit Manager, suivez les procédures décrites ici.

Trouver les commandes disponibles dans AWS Audit Manager

Vous trouverez tous les contrôles disponibles sur la page de la bibliothèque de contrôles de la console Audit Manager.

Vous pouvez également consulter tous les contrôles disponibles à l'aide de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour afficher les contrôles. AWS Audit Manager Les deux politiques suggérées pour accorder ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Audit Manager console

Pour afficher les contrôles disponibles sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation, choisissez Bibliothèque de contrôles.
3. Choisissez un onglet pour parcourir les commandes disponibles.
   - Choisissez Commun pour voir les contrôles communs fournis par AWS.
   - Choisissez Standard pour voir les commandes standard fournies par AWS.
   - Choisissez Personnalisé pour voir les contrôles personnalisés que vous avez créés.

AWS CLI

Pour trouver les commandes communes dans le (AWS CLI

Exécutez la list-common-controlscommande pour afficher la liste des contrôles courants.

```
aws controlcatalog list-common-controls
```

Vous pouvez également utiliser l'`common-control-filter`attribut facultatif pour renvoyer une liste de contrôles courants ayant un objectif spécifique.

Dans l'exemple suivant, remplacez le *`texte de l'espace réservé`* par vos propres informations.

```
aws controlcatalog list-common-controls --common-control-filter OBJECTIVE-ARN
```

Pour trouver d'autres types de contrôles dans AWS CLI

Exécutez la commande list-controls et spécifiez le `--control-type` as `CustomStandard`, ou. `Core`

Dans l'exemple suivant, remplacez le *`texte de l'espace réservé`* par vos propres informations.

```
aws auditmanager list-controls --control-type Type
```

Audit Manager API

Pour trouver des contrôles courants à l'aide de l'API

Utilisez cette ListCommonControlsopération pour afficher la liste des contrôles courants disponibles. Vous pouvez également utiliser l'`commonControlFilter`attribut facultatif pour renvoyer une liste de contrôles ayant un objectif spécifique.

Pour trouver d'autres types de contrôle à l'aide de l'API

Utilisez l'ListControlsopération et spécifiez le ControlType sous la forme `CustomStandard`, ou`Core`.

Pour plus d'informations, choisissez l'un des liens de la procédure précédente pour en savoir plus dans la référence de l'AWS Audit Manager API. Cela inclut des informations sur la façon d'utiliser ces opérations et paramètres dans l'un des SDK spécifiques au langage AWS .

Étapes suivantes

Lorsque vous êtes prêt à explorer les détails d'un contrôle, suivez les étapes décrites dansRévision d'un contrôle dans AWS Audit Manager. Cette page vous guidera à travers les détails du contrôle et expliquera les informations que vous y voyez.

Sur la page de la bibliothèque de contrôles, vous pouvez également créer un contrôle personnalisé, modifier un contrôle personnalisé ou supprimer un contrôle personnalisé.

Ressources supplémentaires

Pour des solutions aux problèmes de contrôle dans Audit Manager, voirRésolution des problèmes liés aux contrôles et aux ensembles de contrôles.

Révision d'un contrôle dans AWS Audit Manager

Vous pouvez consulter les détails d'un contrôle à l'aide de la console Audit Manager, de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

Pour commencer à examiner un contrôle dans Audit Manager, suivez les procédures décrites ici.

Révision d'un contrôle commun

Lorsque vous devez examiner les détails d'un contrôle, vous trouverez les informations organisées en plusieurs sections sur la page des détails du contrôle. Ces sections vous aident à accéder facilement aux informations pertinentes pour ce contrôle et à les comprendre.

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour consulter les contrôles courants dans Audit Manager. Plus précisément, vous avez besoin des autorisations suivantes pour consulter les contrôles courants, les objectifs de contrôle et les domaines de contrôle fournis par AWS Control Catalog :

- `controlcatalog:ListCommonControls`
- `controlcatalog:ListDomains`
- `controlcatalog:ListObjectives`

Une politique suggérée qui accorde ces autorisations est AWSAuditManagerAdministratorAccess.

Procédure

Vous pouvez consulter un contrôle commun à l'aide de la console Audit Manager, AWS de l'API Control Catalog ou du AWS Command Line Interface (AWS CLI).

Audit Manager console

Pour afficher les détails des contrôles courants sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation, choisissez Bibliothèque de contrôles.
3. Choisissez Commun pour voir les contrôles communs fournis par AWS.

4. Choisissez un nom de contrôle courant pour afficher les détails de ce contrôle.
5. Passez en revue les détails des contrôles courants en utilisant les informations suivantes comme référence.

Section d'aperçu

Cette section décrit le contrôle commun.

Onglet Sources de preuves

Cet onglet contient les informations suivantes :

Name (Nom)	Description
Contrôles de base	Il s'agit des contrôles de base qui collectent des preuves à l'appui du contrôle commun. • Lorsque vous collectez des preuves pour ce contrôle commun, vous collectez automatiquement des preuves pour tous les contrôles de base répertoriés ici. Lorsque chacun de ces contrôles de base est mis en œuvre avec succès, cela permet de démontrer que vous répondez aux exigences du contrôle commun. • Chaque contrôle de base utilise un groupe prédéfini de sources de données pour collecter des preuves concernan t un Service AWS. AWS gère ces sources de données pour vous. Cela signifie qu'ils sont automatiquement mis à jour chaque fois que les réglementations et les normes changent et que de nouvelles sources de données sont identifiées. Choisissez n'importe quel contrôle de base pour voir les sources de données sous-jacentes.

Onglet Exigences associées

Lorsque vous collectez des preuves pour ce contrôle commun, les mêmes preuves peuvent vous aider à démontrer la conformité aux exigences des contrôles standard associés répertoriés dans cet onglet. Choisissez n'importe quelle commande standard pour obtenir plus de détails.

> **Note**
>
> - Le contrôle commun peut produire des preuves qui ne démontrent qu'une conformité partielle à un contrôle standard. Il est possible que vous ayez besoin de preuves supplémentaires pour démontrer le respect total d'un contrôle standard.
> - Pour le moment, l'onglet Exigences associées affiche uniquement les contrôles standard associés. Bien qu'un contrôle commun puisse être associé à un ou plusieurs contrôles personnalisés, ces relations ne sont pas affichées dans cet onglet.

AWS CLI

Pour consulter les détails des contrôles courants dans le AWS CLI

1. Exécutez la list-common-controlscommande pour afficher la liste des contrôles courants disponibles. Lorsque vous utilisez cette opération, vous pouvez appliquer une option `common-control-filter` pour voir les contrôles courants ayant un objectif spécifique.

```
aws controlcatalog list-common-controls
```

2. Dans la réponse, identifiez le contrôle commun que vous souhaitez examiner et prenez note de ses détails.

AWS Control Catalog API

Pour afficher les détails des contrôles courants à l'aide de l'API

1. Utilisez cette ListCommonControlsopération pour afficher la liste des contrôles courants disponibles. Lorsque vous utilisez cette opération, vous pouvez appliquer une option `commonControlFilter` pour afficher la liste des contrôles ayant un objectif spécifique.
2. Dans la réponse, identifiez le contrôle que vous souhaitez examiner et prenez note de ses détails.

Pour plus d'informations sur ces opérations d'API, cliquez sur le lien dans cette procédure pour en savoir plus dans la référence d'API du catalogue de AWS contrôle. Cela inclut des informations

sur la façon d'utiliser ces opérations et paramètres dans l'un des SDK spécifiques au langage AWS .

Étapes suivantes

Vous pouvez choisir les contrôles courants qui représentent vos objectifs et les utiliser comme éléments de base pour créer un contrôle personnalisé. Chaque contrôle commun automatisé correspond à un groupe prédéfini de sources de AWS données qu'Audit Manager gère pour vous. Cela signifie que vous n'avez pas besoin d'être un AWS expert pour savoir quelles sources de données collectent les preuves pertinentes pour vos objectifs. De plus, vous n'êtes pas obligé de gérer vous-même ces mappages de sources de données.

Pour obtenir des instructions sur la façon de créer un contrôle personnalisé utilisant des contrôles courants comme source de preuves, voirCréation d'un contrôle personnalisé dans AWS Audit Manager.

Ressources supplémentaires

- Révision d'un contrôle de base
- Révision d'un contrôle standard
- Révision d'un contrôle personnalisé

Révision d'un contrôle de base

Vous pouvez consulter les détails d'un contrôle de base à l'aide de la console Audit Manager, de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour afficher les contrôles. AWS Audit Manager Les deux politiques suggérées qui accordent ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Audit Manager console

Pour afficher les détails des contrôles de base sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation, choisissez Bibliothèque de contrôles.
3. Choisissez Commun pour voir les contrôles communs fournis par AWS.
4. Recherchez le contrôle commun adapté à votre cas d'utilisation.
5. Choisissez l'icône d'arborescence à côté du nom de contrôle commun. Cela affiche les commandes principales qui prennent en charge le contrôle commun.
6. Choisissez le nom du contrôle principal que vous souhaitez examiner.
7. Passez en revue les détails du contrôle de base en utilisant les informations suivantes comme référence.

Section d'aperçu

Cette section décrit le contrôle de base et répertorie les types de sources de données à partir desquels il collecte des preuves.

Onglet Sources de preuves

Cet onglet contient les informations suivantes :

Name (Nom)	Description
Sources de données	Il s'agit des sources de données AWS gérées à partir desquelles le contrôle central recueille des preuves. Ces sources de données sont automatiquement mises à jour chaque fois que les réglementations et les normes changent et que de nouvelles sources de données sont identifiées. • Cartographie : mot clé spécifique utilisé pour collecter des preuves. • Si c'est le cas AWS Config, le mappage est une AWS Config règle (telle que`SNS_ENCRYPTED_KMS`).

Name (Nom)	Description
	• Si c'est le cas AWS Security Hub, le mappage est un contrôle Security Hub (tel que`EC2.1`). • Si le type est un appel AWS d'API, le mappage est un appel d'API (tel que`kms_ListKeys`). • Si c'est le cas AWS CloudTrail, le mappage est un CloudTrail événement (tel que`CreateAccessKey`). • Type : type de source de données d'où proviennent les preuves. • Si Audit Manager collecte les preuves, le type peut être AWS Security Hub, AWS ConfigAWS CloudTrail, ou des appels AWS d'API. • Si vous téléchargez vos propres preuves, le type est Manuel. Une description indique si l'élément probant manuel requis est un Chargement de fichier ou une Réponse sous forme de texte. • Fréquence : fréquence à laquelle Audit Manager collecte des preuves relatives à une source de données d'appel d' AWS API.

Onglet Détails

Cet onglet contient les informations suivantes :

Name (Nom)	Description
Instructions	Les instructions qui décrivent comment tester et corriger le contrôle.
Informations sur les tests	Les procédures de test recommandées.
Plan d'action	Les mesures recommandées à prendre si vous devez corriger le contrôle.

AWS CLI

Pour consulter les détails des commandes de base dans AWS CLI

1. Suivez les étapes pour trouver un contrôle. Assurez-vous de définir le `--control-type` comme et `Core` d'appliquer les filtres facultatifs nécessaires.

```
aws auditmanager list-controls --control-type Core
```

2. Dans la réponse, identifiez le contrôle que vous souhaitez examiner et prenez note de l'ID de contrôle et du nom de ressource Amazon (ARN).
3. Exécutez la commande get-control et spécifiez le. `--control-id` Dans l'exemple suivant, remplacez *`le texte de l'espace réservé`* par vos propres informations.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> Les détails du contrôle sont renvoyés au format JSON. Pour vous aider à comprendre ces données, voir get-control Output dans le manuel de référence des AWS CLI commandes.

4. Pour voir les détails des balises, exécutez la list-tags-for-resourcecommande et spécifiez le`--resource-arn`. Dans l'exemple suivant, remplacez le *`texte de l'espace réservé`* par vos propres informations.

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Pour afficher les détails du contrôle de base à l'aide de l'API

1. Suivez les étapes pour trouver un contrôle. Assurez-vous de définir le ControlType comme tel `Core` et d'appliquer les filtres facultatifs nécessaires.
2. Dans la réponse, identifiez le contrôle que vous souhaitez examiner et prenez note de l'ID de contrôle et du nom de ressource Amazon (ARN).

3. Utilisez l'GetControlopération et spécifiez le ControlID que vous avez noté à l'étape 2.

   > **Tip**
   >
   > Les détails du contrôle sont renvoyés au format JSON. Pour vous aider à comprendre ces données, consultez la section Éléments de GetControl réponse dans la référence de l'AWS Audit Manager API.

4. Pour voir les détails de la balise, utilisez l'ListTagsForResourceopération et spécifiez le ResourceArn que vous avez noté à l'étape 2.

Pour plus d'informations sur ces opérations d'API, cliquez sur l'un des liens de cette procédure pour en savoir plus dans la référence des AWS Audit Manager API. Cela inclut des informations sur la façon d'utiliser ces opérations et paramètres dans l'un des SDK spécifiques au langage AWS .

Étapes suivantes

Vous pouvez choisir les contrôles de base qui représentent vos objectifs et les utiliser comme éléments de base pour créer un contrôle personnalisé. Chaque contrôle central automatisé correspond à un groupe prédéfini de sources de AWS données qu'Audit Manager gère pour vous. Cela signifie que vous n'avez pas besoin d'être un AWS expert pour savoir quelles sources de données collectent les preuves pertinentes pour vos objectifs. De plus, vous n'êtes pas obligé de gérer vous-même ces mappages de sources de données.

Pour obtenir des instructions sur la façon de créer un contrôle personnalisé qui utilise les contrôles de base comme source de preuves, voirCréation d'un contrôle personnalisé dans AWS Audit Manager.

Ressources supplémentaires

- Révision d'un contrôle commun
- Révision d'un contrôle standard
- Révision d'un contrôle personnalisé

Révision d'un contrôle standard

Vous pouvez consulter les détails d'un contrôle standard à l'aide de la console Audit Manager, de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour afficher les contrôles. AWS Audit Manager Les deux politiques suggérées qui accordent ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Vous pouvez consulter les détails d'un contrôle standard à l'aide de la console Audit Manager, de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

Audit Manager console

Pour afficher les détails des contrôles standard sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation, choisissez Bibliothèque de contrôles.
3. Choisissez Standard pour voir les commandes standard fournies par AWS.
4. Choisissez un nom de contrôle standard pour afficher les détails de ce contrôle.
5. Passez en revue les détails du contrôle standard en utilisant les informations suivantes comme référence.

Section d'aperçu

Cette section décrit le contrôle standard et répertorie les types de sources de données qu'il utilise pour collecter des preuves.

Onglet Sources de preuves

Cet onglet contient les informations suivantes :

Name (Nom)	Description
Contrôles de base	Il s'agit des contrôles de base qui collectent des preuves à l'appui du contrôle standard.

Name (Nom)	Description
	Chaque contrôle de base utilise un groupe prédéfini de sources de données pour collecter des preuves concernant un Service AWS. Ces sources de données sont gérées pour vous par AWS et sont automatiquement mises à jour chaque fois que les réglementations et les normes changent et que de nouvelles sources de données sont identifiées. Choisisse z n'importe quel contrôle de base pour voir les sources de données sous-jacentes.

Sources de données	Il s'agit des autres sources de données AWS gérées qui collectent des preuves à l'appui du contrôle standard.
	• Cartographie : mot clé spécifique utilisé pour collecter des preuves.
	  • Si c'est le cas AWS Config, le mappage est une AWS Config règle (telle que`SNS_ENCRYPTED_KMS`).
	  • Si c'est le cas AWS Security Hub, le mappage est un contrôle Security Hub (tel que`EC2.1`).
	  • Si le type est un appel AWS d'API, le mappage est un appel d'API (tel que`kms_ListKeys`).
	  • Si c'est le cas AWS CloudTrail, le mappage est un CloudTrail événement (tel que`CreateAccessKey`).
	• Type : type de source de données d'où proviennent les preuves.
	  • Si Audit Manager collecte les preuves, le type peut être AWS Security Hub, AWS ConfigAWS CloudTrail, ou des appels AWS d'API.
	  • Si vous téléchargez vos propres preuves, le type est Manuel. Une description indique si l'élément probant manuel requis est un Chargement de fichier ou une Réponse sous forme de texte.
	• Fréquence : fréquence à laquelle Audit Manager collecte des preuves relatives à une source de données d'appel d' AWS API.

Onglet Détails

Cet onglet contient les informations suivantes :

Name (Nom)	Description
Instructions	Les instructions qui décrivent comment tester et corriger le contrôle.
Informations sur les tests	Les procédures de test recommandées.
Plan d'action	Les mesures recommandées à prendre si vous devez corriger le contrôle.
Balises	Les balises associées au contrôle.
Clé	La clé de balise (par exemple, une norme de conformité, une réglementation ou une catégorie).
Valeur	Valeur de balise.

AWS CLI

Pour consulter les détails des commandes standard dans AWS CLI

1. Suivez les étapes pour trouver un contrôle. Assurez-vous de définir le `--control-type` comme et `Standard` d'appliquer les filtres facultatifs nécessaires.

```
aws auditmanager list-controls --control-type Standard
```

2. Dans la réponse, identifiez le contrôle que vous souhaitez examiner et prenez note de l'ID de contrôle et du nom de ressource Amazon (ARN).
3. Exécutez la commande get-control et spécifiez le. `--control-id` Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> Les détails du contrôle sont renvoyés au format JSON. Pour vous aider à comprendre ces données, voir get-control Output dans le manuel de référence des AWS CLI commandes

4. Pour voir les détails des balises, exécutez la list-tags-for-resourcecommande et spécifiez le`--resource-arn`. Dans l'exemple suivant, remplacez le *`texte de l'espace réservé`* par vos propres informations.

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Pour afficher les détails des contrôles standard à l'aide de l'API

1. Suivez les étapes pour trouver un contrôle. Assurez-vous de définir le ControlType comme tel `Standard` et d'appliquer les filtres facultatifs nécessaires.
2. Dans la réponse, identifiez le contrôle que vous souhaitez examiner et prenez note de l'ID de contrôle et du nom de ressource Amazon (ARN).
3. Utilisez l'GetControlopération et spécifiez le ControlID que vous avez noté à l'étape 2.

> **Tip**
>
> Les détails du contrôle sont renvoyés au format JSON. Pour vous aider à comprendre ces données, consultez la section Éléments de GetControl réponse dans la référence de l'AWS Audit Manager API.

4. Pour voir les détails de la balise, utilisez l'ListTagsForResourceopération et spécifiez le ResourceArn que vous avez noté à l'étape 2.

Pour plus d'informations sur ces opérations d'API, cliquez sur l'un des liens de cette procédure pour en savoir plus dans la référence des AWS Audit Manager API. Cela inclut des informations sur la façon d'utiliser ces opérations et paramètres dans l'un des SDK spécifiques au langage AWS .

Étapes suivantes

Vous pouvez ajouter un contrôle standard à n'importe lequel de vos frameworks personnalisés. Pour obtenir des instructions, veuillez consulter Création d'un framework personnalisé dans AWS Audit Manager.

Vous pouvez également personnaliser n'importe quel contrôle standard afin qu'il réponde à vos besoins. Pour obtenir des instructions, veuillez consulter Création d'une copie modifiable d'un contrôle dans AWS Audit Manager.

Ressources supplémentaires

- Révision d'un contrôle commun
- Révision d'un contrôle de base
- Révision d'un contrôle personnalisé

Révision d'un contrôle personnalisé

Vous pouvez consulter les détails d'un contrôle personnalisé à l'aide de la console Audit Manager, de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour afficher les contrôles. AWS Audit Manager Les deux politiques suggérées qui accordent ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Vous pouvez consulter les détails d'un contrôle personnalisé à l'aide de la console Audit Manager, de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

Audit Manager console

Pour afficher les détails des contrôles personnalisés sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.

2. Dans le panneau de navigation, choisissez Bibliothèque de contrôles.
3. Choisissez Personnalisé pour voir les contrôles personnalisés que vous avez créés.
4. Choisissez un nom de contrôle personnalisé pour afficher les détails de ce contrôle.
5. Passez en revue les détails du contrôle personnalisé en utilisant les informations suivantes comme référence.

Section d'aperçu

Cette section décrit le contrôle personnalisé et répertorie les types de sources de données qu'il utilise pour collecter des preuves. Il fournit également des informations sur la date de création et de dernière mise à jour du contrôle.

Onglet Sources de preuves

Cet onglet indique d'où le contrôle personnalisé collecte les preuves. Il contient les informations suivantes :

Name (Nom)	Description
Contrôles communs	Il s'agit des contrôles courants qui collectent des preuves à l'appui du contrôle personnalisé. Les contrôles courants collectent des preuves à l'aide de sources de données sous-jacentes AWS gérées pour vous. Pour chaque contrôle commun répertorié, Audit Manager collecte les preuves pertinentes pour tous les contrôles de base sous-jacents. Choisissez un contrôle commun pour voir les contrôles principaux associés.
Contrôles de base	Il s'agit des contrôles de base qui collectent des preuves à l'appui du contrôle personnalisé. Les contrôles de base collectent des preuves à l'aide d'un groupe prédéfini de sources de données qui se AWS gèrent pour vous. Choisissez un contrôle principal pour voir les sources de données sous-jacentes.
Sources de données	Il s'agit des sources de données qui collectent des preuves à l'appui du contrôle personnalisé.

Name (Nom)	Description

	Note
	Ces sources de données ne sont pas gérées pour vous par AWS. Vous êtes responsable de leur maintenance.
	
	• Nom : nom de la source de données.
	• Type : type de source de données d'où proviennent les preuves.
	  • Si Audit Manager collecte les preuves, le type peut être AWS Security Hub, AWS ConfigAWS CloudTrail, ou des appels AWS d'API.
	  • Si vous téléchargez vos propres preuves, le type est Manuel. Une description indique si l'élément probant manuel requis est un Chargement de fichier ou une Réponse sous forme de texte.
	• Cartographie : mot clé spécifique utilisé pour collecter des preuves.
	  • Si c'est le cas AWS Config, le mappage est une AWS Config règle (telle que`SNS_ENCRYPTED_KMS`).
	  • Si c'est le cas AWS Security Hub, le mappage est un contrôle Security Hub (tel que`EC2.1`).
	  • Si le type est un appel AWS d'API, le mappage est un appel d'API (tel que`kms_ListKeys`).
	  • Si c'est le cas AWS CloudTrail, le mappage est un CloudTrail événement (tel que`CreateAccessKey`).
	• Fréquence : fréquence à laquelle Audit Manager collecte des preuves relatives à une source de données d'appel d' AWS API.

Onglet Détails

Cet onglet contient les informations suivantes :

Name (Nom)	Description
Instructions	Les instructions qui décrivent comment tester et corriger le contrôle.
Informations sur les tests	Les procédures de test recommandées.
Plan d'action	Les mesures recommandées à prendre si vous devez corriger le contrôle.
Balises	Les balises associées au contrôle.
Clé	La clé de balise (par exemple, une norme de conformité, une réglementation ou une catégorie).
Valeur	Valeur de balise.

AWS CLI

Pour afficher les détails des contrôles personnalisés dans AWS CLI

1. Suivez les étapes pour trouver un contrôle. Assurez-vous de définir le `--control-type` comme et `Custom` d'appliquer les filtres facultatifs nécessaires.

```
aws auditmanager list-controls --control-type Custom
```

2. Dans la réponse, identifiez le contrôle que vous souhaitez examiner et prenez note de l'ID de contrôle et du nom de ressource Amazon (ARN).
3. Exécutez la commande get-control et spécifiez le. `--control-id` Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations.

```
aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Tip**
>
> Les détails du contrôle sont renvoyés au format JSON. Pour vous aider à comprendre ces données, voir get-control Output dans le manuel de référence des AWS CLI commandes.

4. Pour voir les balises d'un contrôle, utilisez la list-tags-for-resourcecommande et spécifiez le`--resource-arn`. Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations :

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Audit Manager API

Pour afficher les détails des contrôles personnalisés à l'aide de l'API

1. Suivez les étapes pour trouver un contrôle. Assurez-vous de définir le ControlType comme tel `Custom` et d'appliquer les filtres facultatifs nécessaires.
2. Dans la réponse, identifiez le contrôle que vous souhaitez vérifier et prenez note de l'ID du contrôle et de son Amazon Resource Name (ARN).
3. Utilisez l'GetControlopération et spécifiez le ControlID que vous avez noté à l'étape 2.

> **Tip**
>
> Les détails du contrôle sont renvoyés au format JSON. Pour vous aider à comprendre ces données, consultez la section Éléments de GetControl réponse dans la référence de l'AWS Audit Manager API.

4. Pour voir les balises du contrôle, utilisez l'ListTagsForResourceopération et spécifiez le ResourceArn du contrôle que vous avez noté à l'étape 2.

Pour plus d'informations sur ces opérations d'API, cliquez sur l'un des liens de cette procédure pour en savoir plus dans la référence des AWS Audit Manager API. Cela inclut des informations sur la façon d'utiliser ces opérations et paramètres dans l'un des SDK spécifiques au langage AWS .

Étapes suivantes

Vous pouvez ajouter un contrôle personnalisé à n'importe lequel de vos frameworks personnalisés. Pour obtenir des instructions, veuillez consulter Création d'un framework personnalisé dans AWS Audit Manager.

Vous pouvez également modifier un contrôle personnalisé, créer une copie modifiable d'un contrôle personnalisé ou supprimer un contrôle personnalisé dont vous n'avez plus besoin.

Ressources supplémentaires

- Révision d'un contrôle commun
- Révision d'un contrôle de base
- Révision d'un contrôle standard

Création d'un contrôle personnalisé dans AWS Audit Manager

Vous pouvez utiliser des contrôles personnalisés pour recueillir des preuves répondant à vos besoins spécifiques en matière de conformité.

Tout comme les contrôles standard, les contrôles personnalisés collectent des éléments probants en permanence lorsqu'ils sont actifs dans vos évaluations. Vous pouvez également ajouter des éléments probants manuels aux contrôles personnalisés que vous créez. Chaque élément probant devient un enregistrement qui vous aide à démontrer la conformité aux exigences de votre contrôle personnalisé.

Pour commencer, voici quelques exemples de la façon dont vous pouvez utiliser des contrôles personnalisés :

Associez les contrôles de votre entreprise à des groupes prédéfinis de sources de AWS données

> Vous pouvez intégrer les contrôles de votre entreprise à Audit Manager en utilisant les contrôles courants comme source de preuves. Choisissez les contrôles courants qui représentent vos objectifs et utilisez-les comme éléments de base pour créer un contrôle qui collecte des preuves concernant l'ensemble de vos besoins en matière de conformité. Chaque contrôle commun automatisé correspond à un groupe prédéfini de sources de données. Cela signifie que vous n'avez pas besoin d'être un AWS expert pour savoir quelles sources de données collectent les

preuves pertinentes pour vos objectifs. Et lorsque vous utilisez des contrôles courants comme source de preuves, vous n'avez plus besoin de gérer les mappages des sources de données, car Audit Manager s'en charge pour vous.

Créer une question d'évaluation des risques liés aux fournisseurs

Vous pouvez utiliser des contrôles personnalisés pour faciliter la gestion des évaluations des risques liés aux fournisseurs. Chaque contrôle que vous créez peut représenter une question d'évaluation des risques individuelle. Par exemple, le nom du contrôle peut être une question, et vous pouvez fournir une réponse en téléchargeant un fichier ou en saisissant une réponse textuelle comme preuve manuelle.

Points clés

Pour créer des contrôles personnalisés dans Audit Manager, vous avez le choix entre deux méthodes :

1. Création d'un contrôle à partir de zéro - Cette méthode offre une flexibilité maximale et vous permet d'adapter le contrôle à vos besoins exacts. C'est une bonne option lorsque vous avez une exigence de conformité spécifique qui n'est pas couverte de manière adéquate par un contrôle existant. Cette méthode est particulièrement utile lorsque vous devez mapper les contrôles d'entreprise de votre organisation à des groupes prédéfinis de sources de AWS données ou lorsque vous souhaitez créer des questions d'évaluation des risques fournisseurs sous forme de contrôles individuels.
2. Création d'une copie modifiable d'un contrôle existant : si un contrôle standard ou personnalisé existant répond partiellement à vos besoins, vous pouvez créer une copie modifiable de ce contrôle. Cette approche est plus efficace si vous ne devez apporter que des modifications mineures à un contrôle existant. C'est une bonne option si vous souhaitez ajuster quelques attributs afin de mieux adapter le contrôle à vos besoins spécifiques. Par exemple, vous pouvez modifier la fréquence à laquelle un contrôle utilise un appel d'API pour collecter des preuves, puis modifier le nom du contrôle en conséquence.

Ressources supplémentaires

Pour obtenir des instructions sur la création d'un contrôle personnalisé, consultez les ressources suivantes.

- Création d'un contrôle personnalisé à partir de zéro dans AWS Audit Manager

- Création d'une copie modifiable d'un contrôle dans AWS Audit Manager

Création d'un contrôle personnalisé à partir de zéro dans AWS Audit Manager

Lorsque les exigences de conformité de votre organisation ne correspondent pas aux contrôles standard prédéfinis disponibles dans AWS Audit Manager, vous pouvez créer votre propre contrôle personnalisé à partir de zéro.

Cette page décrit les étapes à suivre pour créer un contrôle personnalisé adapté à vos besoins spécifiques.

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour créer un contrôle personnalisé dans AWS Audit Manager. Les deux politiques suggérées qui accordent ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Pour collecter des preuves avec succès auprès de AWS Config Security Hub, assurez-vous de suivre les étapes suivantes :

- Activez AWS Config, puis appliquez les paramètres requis pour une utilisation AWS Config avec Audit Manager
- Activez Security Hub, puis appliquez les paramètres requis pour utiliser Security Hub avec Audit Manager

Audit Manager peut ensuite collecter des preuves chaque fois qu'une évaluation a lieu pour une AWS Config règle ou un contrôle Security Hub donné.

Procédure

Tâches

- Étape 1 : définir les détails du contrôle
- Étape 2 : Spécifier les sources de preuves
- Étape 3 (facultatif) : Définir le plan d'action
- Étape 4 : vérifier et créer le contrôle

Étape 1 : définir les détails du contrôle

Commencez par définir les détails de votre contrôle personnalisé.

> **Important**
>
> Nous vous recommandons vivement de ne jamais saisir d'informations d'identification sensibles dans des champs de forme libre tels que les informations de contrôle ou les informations de test. Si vous créez des contrôles personnalisés contenant des informations sensibles, vous ne pouvez partager aucun de vos frameworks personnalisés contenant ces contrôles.

Pour définir les détails du contrôle

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Bibliothèque de contrôles, puis Création d'un contrôle personnalisé.
3. Sous Détails du contrôle, saisissez les informations suivantes concernant le contrôle.
   - Contrôle : saisissez un nom convivial, un titre ou une question d'évaluation des risques. Cette valeur vous permet d'identifier votre contrôle dans la bibliothèque de contrôles.
   - Description (facultatif) : saisissez les détails pour aider les autres à comprendre l'objectif du contrôle. Cette description apparaît sur la page des détails du contrôle.
4. Sous Informations de test, saisissez les étapes recommandées pour tester le contrôle.
5. Sous Balises, choisissez Ajouter une nouvelle balise pour associer une balise au contrôle. Vous pouvez spécifier une clé pour chaque balise qui décrit le mieux le cadre de conformité pris en charge par ce contrôle. La clé de balise est obligatoire et peut être utilisée comme critère de recherche pour rechercher ce contrôle dans la bibliothèque de contrôles.
6. Choisissez Suivant.

Étape 2 : Spécifier les sources de preuves

Ensuite, spécifiez certaines sources de preuves. Une source de preuves détermine l'endroit d'où votre contrôle personnalisé collecte les preuves. Vous pouvez utiliser des sources AWS gérées, des sources gérées par le client ou les deux.

> **Tip**
>
> Nous vous recommandons d'utiliser des sources AWS gérées. Chaque fois qu'une source AWS gérée est mise à jour, les mêmes mises à jour sont automatiquement appliquées à tous les contrôles personnalisés qui utilisent ces sources. Cela signifie que vos contrôles personnalisés collectent des preuves par rapport aux dernières définitions de cette source de preuves.

Si vous ne savez pas quelles options choisir, consultez les exemples suivants et nos recommandations.

Votre rôle	Votre objectif	Source de preuves recommandée
Professionnel de la GRC	Je souhaite recueillir des preuves pour un domaine ou un objectif en particulier	AWS géré (common control) Utilisez un groupe prédéfini de sources de données mappées à un contrôle commun spécifique.
Expert technique	Je souhaite recueillir des preuves concernant les AWS ressources dont je suis responsable	AWS géré (core control) Utilisez un groupe prédéfini de sources de données correspondant à une AWS exigence.
Expert technique	Je souhaite utiliser une AWS Config règle personnalisée pour collecter des preuves	Géré par le client (automati sédata source) Utilisez une source de données personnalisée pour collecter des preuves automatisées spécifiques.
Professionnel de la GRC	Je souhaite recueillir des preuves, telles que des	Géré par le client (manueldata source)

Votre rôle	Votre objectif	Source de preuves recommandée
	documents et des réponses textuelles	Utilisez une source de données personnalisée pour télécharger vos propres preuves manuelles.

Pour spécifier une source AWS gérée (recommandé)

Nous vous recommandons de commencer par choisir une ou plusieurs commandes courantes. Lorsque vous choisissez le contrôle commun qui représente votre objectif, Audit Manager collecte les preuves pertinentes pour tous les contrôles de base sous-jacents. Vous pouvez également choisir des contrôles de base individuels si vous souhaitez collecter des preuves ciblées sur votre AWS environnement.

Pour spécifier une source AWS gérée

1. Accédez à la section des sources AWS gérées de la page.
2. Pour ajouter un contrôle commun, procédez comme suit :
    a. Sélectionnez Utiliser un contrôle commun correspondant à votre objectif de conformité.
    b. Choisissez un contrôle commun dans la liste déroulante.
    c. (Facultatif) Répétez l'étape 2 si nécessaire. Vous pouvez ajouter jusqu'à cinq contrôles courants.
3. Pour supprimer un contrôle commun, choisissez le X à côté du nom du contrôle.
4. Pour ajouter un contrôle de base, procédez comme suit :
    a. Sélectionnez Utiliser un contrôle de base correspondant à une directive prescriptive. AWS
    b. Choisissez un contrôle commun dans la liste déroulante.
    c. (Facultatif) Répétez l'étape 4 si nécessaire. Vous pouvez ajouter jusqu'à 50 contrôles principaux.
5. Pour supprimer un contrôle principal, choisissez le X à côté du nom du contrôle.
6. Pour ajouter des sources de données gérées par le client, procédez comme suit. Sinon, choisissez Next (Suivant).

Pour spécifier une source gérée par le client

Pour collecter des preuves automatisées à partir d'une source de données, vous devez choisir un type de source de données et un mappage de source de données. Ces informations correspondent à votre AWS utilisation et indiquent à l'Audit Manager où collecter les preuves. Si vous souhaitez fournir vos propres preuves, vous choisirez plutôt une source de données manuelle.

> **Note**
>
> Vous êtes responsable de la gestion des mappages de sources de données que vous créez au cours de cette étape.

Pour spécifier une source gérée par le client

1. Accédez à la section Sources gérées par le client de la page.
2. Sélectionnez Utiliser une source de données pour collecter des preuves manuellement ou automatiquement.
3. Choisissez Ajouter.
4. Choisissez l'une des options suivantes :

   - Choisissez des appels AWS d'API, puis choisissez un appel d'API et une fréquence de collecte de preuves.
   - Choisissez un AWS CloudTrail événement, puis un nom d'événement.
   - Choisissez une règle AWS Config gérée, puis un identifiant de règle.
   - Choisissez une règle AWS Config personnalisée, puis un identifiant de règle.
   - Choisissez un AWS Security Hub contrôle, puis un contrôle Security Hub.
   - Choisissez Source de données manuelle, puis choisissez une option :
     - Téléchargement de fichiers : utilisez cette option si le contrôle nécessite de la documentation comme preuve.
     - Réponse textuelle — Utilisez cette option si le contrôle nécessite une réponse à une question d'évaluation des risques.

> **Tip**
>
> Pour plus d'informations sur les types de sources de données automatisées et pour obtenir des conseils de résolution des problèmes, consultezTypes de sources de données pris en charge pour les preuves automatisées.
> Si vous devez valider la configuration de votre source de données auprès d'un expert, choisissez pour le moment la source de données manuelle. Ainsi, vous pouvez créer le contrôle et l'ajouter à un framework dès maintenant, puis le modifier ultérieurement selon vos besoins.

5. Sous Nom de la source de données, entrez un nom descriptif.
6. (Facultatif) Sous Détails supplémentaires, saisissez une description de la source de données et une description du dépannage.
7. Choisissez Add data source.
8. (Facultatif) Pour ajouter une autre source de données, choisissez Ajouter et répétez les étapes 1 à 7. Vous pouvez ajouter jusqu'à 100 sources de données.
9. Pour supprimer une source de données, sélectionnez-la dans le tableau, puis choisissez Supprimer.
10. Lorsque vous avez terminé, choisissez Suivant.

Étape 3 (facultatif) : Définir le plan d'action

Indiquez ensuite les actions à entreprendre si ce contrôle doit être corrigé.

> **Important**
>
> Nous vous recommandons vivement de ne jamais saisir d'informations d'identification sensibles dans des champs de forme libre tels que le plan d'action. Si vous créez des contrôles personnalisés contenant des informations sensibles, vous ne pouvez partager aucun de vos frameworks personnalisés contenant ces contrôles.

Pour définir un plan d'action

1. Sous Titre, saisissez un titre descriptif pour le plan d'action.

2. Sous Instructions, entrez des instructions détaillées pour le plan d'action.
3. Choisissez Suivant.

Étape 4 : vérifier et créer le contrôle

Vérifiez les informations pour le contrôle Pour modifier les informations d'une étape, choisissez Modifier.

Lorsque vous avez terminé, choisissez Créer un contrôle personnalisé.

Étapes suivantes

Après avoir créé un nouveau contrôle personnalisé, vous pouvez l'ajouter à un framework personnalisé. Pour en savoir plus, veuillez consulter les sections Création d'un framework personnalisé dans AWS Audit Manager et Modification d'un framework personnalisé dans AWS Audit Manager.

Après avoir ajouté le contrôle personnalisé à un cadre personnalisé, vous pouvez créer une évaluation et commencer à recueillir des preuves. Pour en savoir plus, veuillez consulter la section Création d'une évaluation dans AWS Audit Manager.

Pour revoir votre contrôle personnalisé ultérieurement, consultezTrouver les commandes disponibles dans AWS Audit Manager. Vous pouvez suivre ces étapes pour localiser votre contrôle personnalisé afin de pouvoir l'afficher, le modifier ou le supprimer.

Ressources supplémentaires

Pour des solutions aux problèmes de contrôle dans Audit Manager, consultezRésolution des problèmes liés aux contrôles et aux ensembles de contrôles.

Création d'une copie modifiable d'un contrôle dans AWS Audit Manager

Au lieu de créer un contrôle personnalisé à partir de zéro, vous pouvez utiliser un contrôle standard ou personnalisé existant comme point de départ et créer une copie modifiable qui répond à vos besoins. Dans ce cas, le contrôle standard existant reste dans la bibliothèque de contrôles et un nouveau contrôle est créé avec vos paramètres personnalisés.

Prérequis

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour créer un framework personnalisé dans AWS Audit Manager. Les deux politiques suggérées qui accordent ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Pour collecter des preuves avec succès auprès de AWS Config Security Hub, assurez-vous de suivre les étapes suivantes :

- Activez AWS Config, puis appliquez les paramètres requis pour une utilisation AWS Config avec Audit Manager.
- Activez Security Hub, puis appliquez les paramètres requis pour utiliser Security Hub avec Audit Manager.

Audit Manager peut ensuite collecter des preuves chaque fois qu'une évaluation a lieu pour une AWS Config règle ou un contrôle Security Hub donné.

Procédure

Tâches

- Étape 1 : définir les détails du contrôle
- Étape 2 : Spécifier les sources de preuves
- Étape 3 (facultatif) : définir un plan d'action
- Étape 4 : vérifier et créer le contrôle

Étape 1 : définir les détails du contrôle

Les détails du contrôle sont hérités du contrôle d'origine. Vérifiez et modifiez ces détails si nécessaire.

> **Important**
>
> Nous vous recommandons vivement de ne jamais saisir d'informations d'identification sensibles dans des champs de forme libre tels que les informations de contrôle ou les informations de test. Si vous créez des contrôles personnalisés contenant des informations

sensibles, vous ne pouvez partager aucun de vos frameworks personnalisés contenant ces contrôles.

Pour définir les détails du contrôle

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation, choisissez Bibliothèque de contrôles.
3. Sélectionnez le contrôle standard ou personnalisé auquel vous souhaitez apporter des modifications, puis choisissez Créer une copie.
4. Spécifiez le nouveau nom du contrôle, puis choisissez Continuer.
5. Sous Détails du contrôle, personnalisez les détails du contrôle selon vos besoins.
6. Sous Informations de test, apportez les modifications nécessaires aux instructions.
7. Sous Balises, personnalisez les balises selon vos besoins.
8. Choisissez Suivant.

Étape 2 : Spécifier les sources de preuves

Les sources de preuves sont héritées du contrôle d'origine. Vous pouvez modifier, ajouter ou supprimer des sources de preuves selon vos besoins.

Pour spécifier une source AWS gérée (recommandé)

> **Tip**
>
> Nous vous recommandons de commencer par choisir une ou plusieurs commandes courantes. Si vous avez des exigences de conformité plus précises, vous pouvez également choisir un ou plusieurs contrôles de base spécifiques.

Pour spécifier une source AWS gérée

1. Dans la AWS section Sources gérées, passez en revue les sélections actuelles et apportez les modifications nécessaires.
2. Pour ajouter un contrôle commun, procédez comme suit :

a. Sélectionnez Utiliser un contrôle commun correspondant à votre objectif de conformité.

b. Choisissez un contrôle commun dans la liste déroulante.

c. (Facultatif) Répétez l'étape 2 si nécessaire. Vous pouvez ajouter jusqu'à cinq contrôles courants.

3. Pour supprimer un contrôle commun, choisissez le X à côté du nom du contrôle.

4. Pour ajouter un contrôle de base, procédez comme suit :

a. Sélectionnez Utiliser un contrôle de base correspondant à une directive prescriptive. AWS

b. Choisissez un contrôle commun dans la liste déroulante.

c. (Facultatif) Répétez l'étape 4 si nécessaire. Vous pouvez ajouter jusqu'à 50 contrôles principaux.

5. Pour supprimer un contrôle principal, choisissez le X à côté du nom du contrôle.

6. Pour modifier les sources de données gérées par le client, procédez comme suit. Sinon, choisissez Next (Suivant).

Pour spécifier une source gérée par le client

Pour collecter des preuves automatisées à partir d'une source de données, vous devez choisir un type de source de données et un mappage de source de données. Ces informations correspondent à votre AWS utilisation et indiquent à l'Audit Manager où collecter les preuves. Si vous souhaitez fournir vos propres preuves, vous choisirez plutôt une source de données manuelle.

> **Note**
>
> Vous êtes responsable de la gestion des mappages de sources de données que vous créez au cours de cette étape.

Pour spécifier une source gérée par le client

1. Sous Sources gérées par le client, passez en revue les sources de données actuelles et apportez les modifications nécessaires.

2. Pour supprimer une source de données, sélectionnez-la dans le tableau et choisissez Supprimer.

3. Pour ajouter une nouvelle source de données, procédez comme suit :

a. Sélectionnez Utiliser une source de données pour collecter des preuves manuellement ou automatiquement.

b. Choisissez Ajouter.

c. Choisissez l'une des options suivantes :

- Choisissez des appels AWS d'API, puis choisissez un appel d'API et une fréquence de collecte de preuves.
- Choisissez un AWS CloudTrail événement, puis un nom d'événement.
- Choisissez une règle AWS Config gérée, puis un identifiant de règle.
- Choisissez une règle AWS Config personnalisée, puis un identifiant de règle.
- Choisissez un AWS Security Hub contrôle, puis un contrôle Security Hub.
- Choisissez Source de données manuelle, puis choisissez une option :
  - Téléchargement de fichiers : utilisez cette option si le contrôle nécessite de la documentation comme preuve.
  - Réponse textuelle — Utilisez cette option si le contrôle nécessite une réponse à une question d'évaluation des risques.

> **Tip**
>
> Pour plus d'informations sur les types de sources de données automatisées et pour obtenir des conseils de résolution des problèmes, consultezTypes de sources de données pris en charge pour les preuves automatisées.
> Si vous devez valider la configuration de votre source de données auprès d'un expert, choisissez pour le moment la source de données manuelle. Ainsi, vous pouvez créer le contrôle et l'ajouter à un framework dès maintenant, puis le modifier ultérieurement selon vos besoins.

d. Sous Nom de la source de données, entrez un nom descriptif.

e. (Facultatif) Sous Détails supplémentaires, saisissez une description de la source de données et une description du dépannage.

f. Choisissez Add data source.

g. (Facultatif) Pour ajouter une autre source de données, choisissez Ajouter et répétez l'étape 3. Vous pouvez ajouter jusqu'à 100 sources de données.

4. Lorsque vous avez terminé, choisissez Suivant.

Étape 3 (facultatif) : définir un plan d'action

Le plan d'action est hérité du contrôle initial. Vous pouvez modifier ce plan d'action selon vos besoins.

> **Important**
>
> Nous vous recommandons vivement de ne jamais saisir d'informations d'identification sensibles dans des champs de forme libre tels que le plan d'action. Si vous créez des contrôles personnalisés contenant des informations sensibles, vous ne pouvez partager aucun de vos frameworks personnalisés contenant ces contrôles.

Pour spécifier des instructions

1. Sous Titre, passez en revue le titre et apportez les modifications nécessaires.
2. Sous Instructions, passez en revue les instructions et apportez les modifications nécessaires.
3. Choisissez Suivant.

Étape 4 : vérifier et créer le contrôle

Vérifiez les informations pour le contrôle Pour modifier les informations d'une étape, choisissez Modifier. Lorsque vous avez terminé, choisissez Créer un contrôle personnalisé.

Étapes suivantes

Après avoir créé un nouveau contrôle personnalisé, vous pouvez l'ajouter à un framework personnalisé. Pour en savoir plus, veuillez consulter les sections Création d'un framework personnalisé dans AWS Audit Manager et Modification d'un framework personnalisé dans AWS Audit Manager.

Après avoir ajouté un contrôle personnalisé à un cadre personnalisé, vous pouvez créer une évaluation et commencer à recueillir des preuves. Pour en savoir plus, veuillez consulter la section Création d'une évaluation dans AWS Audit Manager.

Pour revoir votre contrôle personnalisé ultérieurement, consultezTrouver les commandes disponibles dans AWS Audit Manager. Vous pouvez suivre ces étapes pour localiser votre contrôle personnalisé afin de pouvoir l'afficher, le modifier ou le supprimer.

Ressources supplémentaires

Pour des solutions aux problèmes de contrôle dans Audit Manager, consultezRésolution des problèmes liés aux contrôles et aux ensembles de contrôles.

Modification d'un contrôle personnalisé dans AWS Audit Manager

Il se peut que vous deviez modifier vos contrôles personnalisés en fonction de AWS Audit Manager l'évolution de vos exigences de conformité.

Cette page décrit les étapes à suivre pour modifier les détails d'un contrôle personnalisé, les sources de preuves et les instructions du plan d'action.

Prérequis

La procédure suivante suppose que vous avez déjà créé un contrôle personnalisé.

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour modifier un contrôle personnalisé dans AWS Audit Manager. Les deux politiques suggérées qui accordent ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Procédez comme suit pour modifier un contrôle personnalisé.

> **Note**
>
> Lorsque vous modifiez un contrôle, vos modifications sont appliquées à toutes les évaluations dans lesquelles le contrôle est actif. Dans toutes ces évaluations, l'Audit Manager commencera automatiquement à collecter des preuves conformément à la dernière définition de contrôle.

Tâches

- Étape 1 : modifier les détails du contrôle
- Étape 2 : Modifier les sources de preuves
- Étape 3 : modifier le plan d'action

Étape 1 : modifier les détails du contrôle

Passez en revue et modifiez les détails du contrôle selon vos besoins.

> **Important**
>
> Nous vous recommandons vivement de ne jamais saisir d'informations d'identification sensibles dans des champs de forme libre tels que les informations de contrôle ou les informations de test. Si vous créez des contrôles personnalisés contenant des informations sensibles, vous ne pouvez partager aucun de vos frameworks personnalisés contenant ces contrôles.

Modifier les détails d'un contrôle

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez la bibliothèque de contrôle, puis l'onglet Personnaliser.
3. Sélectionnez le compte que vous souhaitez modifier puis choisissez Modifier.
4. Sous Détails du contrôle, modifiez les détails du contrôle selon vos besoins.
5. Sous Informations de test, modifiez la description selon vos besoins.
6. Choisissez Suivant.

Étape 2 : Modifier les sources de preuves

Vous pouvez ensuite modifier, supprimer ou ajouter des sources de preuves pour le contrôle.

> **Note**
>
> Lorsque vous modifiez un contrôle pour inclure plus ou moins de sources de preuves, cela peut affecter la quantité de preuves que votre contrôle collecte dans les évaluations où il

est actif. Par exemple, si vous ajoutez des sources de preuves, vous remarquerez peut-être qu'Audit Manager effectue davantage d'évaluations des ressources et collecte davantage de preuves qu'auparavant. Si vous supprimez les sources de preuves, il est probable que votre contrôle collectera moins de preuves à l'avenir.
Pour plus d'informations sur les évaluations des ressources et la tarification, consultez la section AWS Audit Manager Tarification.

Pour modifier une source AWS gérée

Pour modifier une source AWS gérée

1. Dans la AWS section Sources gérées, passez en revue les sélections actuelles et apportez les modifications nécessaires.
2. Pour ajouter un contrôle commun, procédez comme suit :
   a. Sélectionnez Utiliser un contrôle commun correspondant à votre objectif de conformité.
   b. Choisissez un contrôle commun dans la liste déroulante.
   c. (Facultatif) Répétez l'étape 2 si nécessaire. Vous pouvez ajouter jusqu'à cinq contrôles courants.
3. Pour supprimer un contrôle commun, choisissez le X à côté du nom du contrôle.
4. Pour ajouter un contrôle de base, procédez comme suit :
   a. Sélectionnez Utiliser un contrôle de base correspondant à une directive prescriptive. AWS
   b. Choisissez un contrôle commun dans la liste déroulante.
   c. (Facultatif) Répétez l'étape 4 si nécessaire. Vous pouvez ajouter jusqu'à 50 contrôles principaux.
5. Pour supprimer un contrôle principal, choisissez le X à côté du nom du contrôle.
6. Pour ajouter des sources de données gérées par le client, procédez comme suit. Sinon, choisissez Next (Suivant).

Pour modifier une source gérée par le client

> **Note**
>
> Vous êtes responsable de la gestion des mappages de sources de données que vous modifiez au cours de cette étape.

Pour modifier une source gérée par le client

1. Sous Sources gérées par le client, passez en revue les sources de données actuelles et apportez les modifications nécessaires.
2. Pour supprimer une source de données, sélectionnez-la dans le tableau, puis choisissez Supprimer.
3. Pour ajouter une nouvelle source de données, procédez comme suit :

    a. Sélectionnez Utiliser une source de données pour collecter des preuves manuellement ou automatiquement.

    b. Choisissez Ajouter.

    c. Choisissez l'une des options suivantes :

    - Choisissez des appels AWS d'API, puis choisissez un appel d'API et une fréquence de collecte de preuves.
    - Choisissez un AWS CloudTrail événement, puis un nom d'événement.
    - Choisissez une règle AWS Config gérée, puis un identifiant de règle.
    - Choisissez une règle AWS Config personnalisée, puis un identifiant de règle.
    - Choisissez un AWS Security Hub contrôle, puis un contrôle Security Hub.
    - Choisissez Source de données manuelle, puis choisissez une option :
        - Téléchargement de fichiers : utilisez cette option si le contrôle nécessite de la documentation comme preuve.
        - Réponse textuelle — Utilisez cette option si le contrôle nécessite une réponse à une question d'évaluation des risques.

> **Tip**
>
> Pour plus d'informations sur les types de sources de données automatisées et pour obtenir des conseils de résolution des problèmes, consultezTypes de sources de données pris en charge pour les preuves automatisées.
> Si vous devez valider la configuration de votre source de données auprès d'un expert, choisissez pour le moment la source de données manuelle. Ainsi, vous pouvez créer le contrôle et l'ajouter à un framework dès maintenant, puis le modifier ultérieurement selon vos besoins.

d. Sous Nom de la source de données, entrez un nom descriptif.

e. (Facultatif) Sous Détails supplémentaires, saisissez une description de la source de données et une description du dépannage.

f. Choisissez Add data source.

g. (Facultatif) Pour ajouter une autre source de données, choisissez Ajouter et répétez l'étape 3. Vous pouvez ajouter jusqu'à 100 sources de données.

4. Lorsque vous avez terminé, choisissez Suivant.

Étape 3 : modifier le plan d'action

Ensuite, passez en revue et modifiez le plan d'action facultatif.

> **Important**
>
> Nous vous recommandons vivement de ne jamais saisir d'informations d'identification sensibles dans des champs de forme libre tels que le plan d'action. Si vous créez des contrôles personnalisés contenant des informations sensibles, vous ne pouvez partager aucun de vos frameworks personnalisés contenant ces contrôles.

Pour modifier un plan d'action

1. Sous Titre, modifiez le titre selon vos besoins.
2. Sous Instructions, modifiez les instructions selon vos besoins.
3. Choisissez Suivant.

Étape 4 : Vérifiez et enregistrez

Vérifiez les informations pour le contrôle Pour modifier les informations d'une étape, choisissez Modifier.

Lorsque vous avez terminé, sélectionnez Enregistrer les modifications.

> **Note**
>
> Une fois que vous avez modifié un contrôle, les modifications prennent effet comme suit dans toutes les évaluations actives qui comprennent le contrôle :
>
> - Pour les contrôles utilisant des appels d'API AWS comme type de source de données, les modifications prennent effet à 00 h 00 UTC le jour suivant.
> - Pour tous les autres contrôles, les modifications prennent effet immédiatement.

Étapes suivantes

Lorsque vous êtes certain de ne plus avoir besoin d'un contrôle personnalisé, vous pouvez nettoyer votre environnement Audit Manager en supprimant le contrôle. Pour obtenir des instructions, veuillez consulter Suppression d'un contrôle personnalisé dans AWS Audit Manager.

Ressources supplémentaires

Pour des solutions aux problèmes de contrôle dans Audit Manager, consultezRésolution des problèmes liés aux contrôles et aux ensembles de contrôles.

Modifier la fréquence à laquelle un contrôle collecte des preuves

AWS Audit Manager peut recueillir des preuves à partir de diverses sources de données. La fréquence de collecte des preuves dépend du type de source de données utilisée par le contrôle.

Les sections suivantes fournissent plus d'informations sur la fréquence de collecte d'éléments probants pour chaque type de source de données de contrôle et sur la manière de la modifier (le cas échéant).

Rubriques

- Points clés

- Instantanés de configuration issus d'appels d' AWS API
- Contrôles de conformité effectués par AWS Config
- Contrôles de conformité effectués par Security Hub
- Journaux d'activité des utilisateurs provenant de AWS CloudTrail

Points clés

- Pour les appels d'API AWS , Audit Manager collecte des éléments probants à l'aide d'un appel d'API de description à un autre Service AWS. Vous pouvez définir la fréquence de collecte des éléments probants directement dans Audit Manager (pour les contrôles personnalisés uniquement).
- En effet AWS Config, Audit Manager rapporte le résultat d'un contrôle de conformité directement depuis AWS Config. La fréquence suit les déclencheurs définis dans la AWS Config règle.
- Pour AWS Security Hub, Audit Manager rapporte le résultat d'un contrôle de conformité directement depuis Security Hub. La fréquence suit le calendrier de la vérification de Security Hub.
- Car AWS CloudTrail, Audit Manager collecte des preuves en permanence auprès de CloudTrail. Vous ne pouvez pas modifier la fréquence pour ce type d'élément probant.

Instantanés de configuration issus d'appels d' AWS API

> **Note**
>
> Ce qui suit s'applique uniquement aux contrôles personnalisés. Vous ne pouvez pas modifier la fréquence de collecte de preuves pour un contrôle standard.

Si un contrôle personnalisé utilise des appels d' AWS API comme type de source de données, vous pouvez modifier la fréquence de collecte des preuves dans Audit Manager en suivant ces étapes.

Pour modifier la fréquence de collecte des éléments probants pour un contrôle personnalisé avec une source de données d'appel d'API

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Bibliothèque de contrôle, puis sélectionnez l'onglet Personnalisé.

3. Choisissez le contrôle personnalisé que vous souhaitez modifier, puis choisissez Modifier.
4. Sur la page Modifier les détails du contrôle, choisissez Modifier.
5. Sous Sources gérées par le client, recherchez la source de données des appels d'API que vous souhaitez mettre à jour.
6. Sélectionnez la source de données dans le tableau, puis choisissez Supprimer.
7. Choisissez Ajouter.
8. Choisissez les appels AWS d'API.
9. Choisissez le même appel d'API que celui que vous avez supprimé à l'étape 5, puis sélectionnez votre fréquence de collecte de preuves préférée.
10. Sous Nom de la source de données, entrez un nom descriptif.
11. (Facultatif) Sous Détails supplémentaires, saisissez une description de la source de données et une description du dépannage.
12. Choisissez Suivant.
13. Sur la page Modifier un plan d'action, choisissez Suivant.
14. Sur la page Révision et mise à jour, passez en revue les informations relatives au contrôle personnalisé. Pour modifier les informations d'une étape, choisissez Modifier.
15. Lorsque vous avez terminé, sélectionnez Enregistrer les modifications.

Une fois que vous avez modifié un contrôle, les modifications prennent effet à 00h00 UTC le jour suivant dans toutes les évaluations actives qui incluent le contrôle.

Contrôles de conformité effectués par AWS Config

> **Note**
>
> Ce qui suit s'applique aux contrôles standard et aux contrôles personnalisés qui utilisent AWS Config Rules comme source de données.

Si un contrôle est utilisé AWS Config comme type de source de données, vous ne pouvez pas modifier la fréquence de collecte des preuves directement dans Audit Manager. Cela est dû au fait que la fréquence suit les déclencheurs définis dans la AWS Config règle.

Il existe deux types de déclencheurs pour AWS Config Rules :

1. Modifications de configuration : AWS Config exécute des évaluations de la règle lorsque certains types de ressources sont créés, modifiés ou supprimés.
2. Périodique : AWS Config exécute des évaluations de la règle à la fréquence que vous choisissez (par exemple, toutes les 24 heures).

Pour en savoir plus sur les déclencheurs pour AWS Config Rules, consultez la section Types de déclencheurs dans le Guide du AWS Config développeur.

Pour obtenir des instructions sur la façon de gérer AWS Config Rules, consultez la section Gestion de vos AWS Config règles.

Contrôles de conformité effectués par Security Hub

> **Note**
>
> Ce qui suit s'applique aux contrôles standard et aux contrôles personnalisés qui utilisent les contrôles de Security Hub comme source de données.

Si un contrôle utilise Security Hub comme type de source de données, vous ne pouvez pas modifier la fréquence de collecte des éléments probants directement dans Audit Manager. En effet, la fréquence suit le calendrier des vérifications de Security Hub.

- Les contrôles périodiques s'exécutent automatiquement dans les 12 heures suivant la dernière exécution. Vous ne pouvez pas modifier la périodicité.
- Les vérifications déclenchées par une modification s'exécutent lorsque l'état de la ressource associée change. Même si la ressource ne change pas d'état, l'heure de mise à jour des vérifications déclenchées par une modification est actualisée toutes les 18 heures. Cela permet d'indiquer que le contrôle est toujours activé. En général, utilise des règles déclenchées par des modifications chaque fois que c'est possible.

Pour en savoir plus, consultez la section Planification de l'exécution des contrôles de sécurité dans le guide de l'utilisateur AWS Security Hub .

Journaux d'activité des utilisateurs provenant de AWS CloudTrail

> **Note**
>
> Ce qui suit s'applique aux contrôles standard et aux contrôles personnalisés qui utilisent les journaux d'activité des utilisateurs AWS CloudTrail comme source de données.

Vous ne pouvez pas modifier la fréquence de collecte des preuves pour les contrôles qui utilisent les journaux d'activité CloudTrail comme type de source de données. L'Audit Manager collecte ce type de CloudTrail preuves de manière continue. La fréquence est continue car l'activité des utilisateurs peut se produire à tout moment de la journée.

Suppression d'un contrôle personnalisé dans AWS Audit Manager

Si vous avez créé un contrôle personnalisé et que vous n'en avez plus besoin, vous pouvez le supprimer de votre environnement Audit Manager. Cela vous permet de nettoyer votre espace de travail et de vous concentrer sur les commandes personnalisées adaptées à vos tâches et priorités actuelles.

Prérequis

La procédure suivante suppose que vous avez déjà créé un contrôle personnalisé.

Assurez-vous que votre identité IAM dispose des autorisations appropriées pour supprimer un contrôle personnalisé dans AWS Audit Manager. Les deux politiques suggérées qui accordent ces autorisations sont AWSAuditManagerAdministratorAccessetAutoriser l'accès de gestion des utilisateurs à AWS Audit Manager.

Procédure

Vous pouvez supprimer des contrôles personnalisés à l'aide de la console Audit Manager, de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

> **Important**
>
> Lorsque vous supprimez un contrôle personnalisé, cette action le supprime de tous les frameworks (ou évaluations) personnalisés auxquels il est actuellement associé. Par

conséquent, Audit Manager cesse de collecter des éléments probants pour ce contrôle personnalisé dans toutes vos évaluations. Cela comprend les évaluations que vous avez créées avant de supprimer le contrôle personnalisé.

Audit Manager console

Pour supprimer un contrôle personnalisé sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Bibliothèque de contrôles, puis sélectionnez l'onglet Contrôles personnalisés.
3. Sélectionnez le compte que vous souhaitez supprimer, puis choisissez Supprimer.
4. Dans la fenêtre contextuelle qui apparaît, choisissez Supprimer pour confirmer la suppression.

AWS CLI

Pour supprimer un contrôle personnalisé dans AWS CLI

1. Tout d'abord, identifiez le contrôle personnalisé que vous souhaitez supprimer. Pour ce faire, exécutez la commande list-controls et spécifiez le `--control-type` en tant que `Custom`.

   ```
   aws auditmanager list-controls --control-type Custom
   ```

   La réponse renvoie une liste de contrôles personnalisés. Recherchez le contrôle que vous souhaitez supprimer et notez son ID.

2. Exécutez ensuite la commande delete-control et utilisez le paramètre `--control-id` pour indiquer le contrôle que vous souhaitez supprimer.

   Dans l'exemple suivant, remplacez *`le texte de l'espace réservé`* par vos propres informations.

   ```
   aws auditmanager delete-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

Pour supprimer un contrôle personnalisé à l'aide de l'API

1. Utilisez l'ListControlsopération et spécifiez le ControlType commeCustom. Dans la réponse, recherchez le contrôle que vous souhaitez supprimer et notez son ID.
2. Utilisez cette DeleteControlopération pour supprimer le contrôle personnalisé. Dans la demande, utilisez le paramètre ControlID pour indiquer le contrôle que vous souhaitez supprimer.

Pour plus d'informations sur ces opérations d'API, cliquez sur l'un des liens de la procédure précédente pour en savoir plus dans la référence des AWS Audit Manager API. Cela inclut des informations sur la façon d'utiliser ces opérations et paramètres dans l'un des SDK spécifiques au langage AWS .

Ressources supplémentaires

Pour plus d'informations sur la conservation des données dans Audit Manager, consultezSuppression des données d'Audit Manager.

Révision et configuration de vos AWS Audit Manager paramètres

Vous pouvez vérifier et configurer vos AWS Audit Manager paramètres à tout moment pour vous assurer qu'ils répondent à vos besoins spécifiques.

Ce chapitre explique le processus d'accès, de révision et d'ajustement des paramètres de l'Audit Manager step-by-step. En suivant, vous apprendrez comment modifier vos paramètres généraux, vos paramètres d'évaluation et les paramètres de votre outil de recherche de preuves afin de les aligner sur l'évolution de vos objectifs de conformité et de vos exigences commerciales.

Procédure

Pour commencer, suivez ces étapes pour consulter les paramètres de votre Audit Manager. Vous pouvez consulter vos paramètres d'Audit Manager à l'aide de la console Audit Manager, de la AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

Pour consulter vos paramètres

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Choisissez l'onglet qui correspond à votre objectif.

   - Paramètres généraux - Choisissez cet onglet pour revoir et mettre à jour vos paramètres généraux d'Audit Manager.
   - Paramètres d'évaluation - Choisissez cet onglet pour revoir et mettre à jour les paramètres par défaut de vos évaluations.
   - Paramètres de recherche de preuves - Choisissez cet onglet pour consulter et mettre à jour les paramètres de votre outil de recherche de preuves.

Étapes suivantes

Pour personnaliser les paramètres de l'Audit Manager en fonction de votre cas d'utilisation, suivez les procédures décrites ici.

- Paramètres généraux
  - Configuration de vos paramètres de chiffrement des données
  - Ajouter un administrateur délégué
  - Modification d'un administrateur délégué
  - Supprimer un administrateur délégué
  - Désactivation AWS Audit Manager
- Paramètres d'évaluation
  - Configuration de vos propriétaires d'audit par défaut
  - Configuration de la destination par défaut de votre rapport d'évaluation
  - Configuration des notifications de l'Audit Manager
- Paramètres de recherche de preuves
  - Activation de l'outil de recherche d'éléments probants
  - Confirmation du statut de chercheur de preuves
  - Configuration de votre destination d'exportation par défaut pour Evidence Finder
  - Désactivation de l'outil de recherche d'éléments probants

Configuration de vos paramètres de chiffrement des données

Vous pouvez choisir le mode de chiffrement de vos données. AWS Audit Manager Audit Manager crée automatiquement un fichier unique Clé gérée par AWS pour le stockage sécurisé de vos données. Par défaut, vos données Audit Manager sont chiffrées avec cette clé KMS. Toutefois, si vous souhaitez personnaliser vos paramètres de chiffrement des données, vous pouvez spécifier votre propre clé de chiffrement symétrique gérée par le client. L'utilisation de votre propre clé KMS vous donne plus de flexibilité dans la mesure où elle vous permet de créer, modifier ou désactiver des clés.

Prérequis

Si vous fournissez une clé gérée par le client, elle doit être Région AWS identique à celle de votre évaluation afin de générer des rapports d'évaluation et d'exporter avec succès les résultats de recherche de preuves.

Procédure

Vous pouvez mettre à jour vos paramètres de chiffrement des données à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

> **Note**
>
> Lorsque vous modifiez vos paramètres de chiffrement des données d'Audit Manager, ces modifications s'appliquent à n'importe quelles nouvelles évaluations que vous créez. Cela inclut tous les rapports d'évaluation et les exportations de recherche d'éléments probants que vous créez à partir de vos nouvelles évaluations.
>
> Les modifications ne s'appliquent pas aux évaluations existantes que vous avez créées avant de modifier vos paramètres de chiffrement. Cela inclut les nouveaux rapports d'évaluation et les exportations CSV que vous créez à partir d'évaluations existantes, en plus des rapports d'évaluation et des exportations CSV existants. Les évaluations existantes, ainsi que tous leurs rapports d'évaluation et exportations CSV, continuent d'utiliser l'ancienne clé KMS. Si l'identité IAM qui génère le rapport d'évaluation ne peut pas utiliser l'ancienne clé KMS, vous pouvez accorder des autorisations au niveau de la stratégie de clé.

Audit Manager console

Pour mettre à jour vos paramètres de chiffrement des données sur la console Audit Manager

1. Dans l'onglet Paramètres généraux, accédez à la section Chiffrement des données.
2. Pour utiliser la clé KMS par défaut fournie par Audit Manager, décochez la case Personnaliser les paramètres de chiffrement (avancés).
3. Pour utiliser une clé gérée par le client, sélectionnez la case Personnaliser les paramètres de chiffrement (avancé). Choisissez alors une clé KMS existante ou créez-en une.

AWS CLI

Pour mettre à jour vos paramètres de chiffrement des données dans AWS CLI

Exécutez la commande paramètres de mise à jour et utilisez le paramètre `--kms-key` pour préciser votre propre clé gérée par le client.

Dans l'exemple suivant, remplacez *`le texte de l'espace réservé`* par vos propres informations.

```
aws auditmanager update-settings --kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Audit Manager API

Pour mettre à jour vos paramètres de chiffrement des données à l'aide de l'API

Appelez l'UpdateSettingsopération et utilisez le paramètre KMSKey pour spécifier votre propre clé gérée par le client.

Pour plus d'informations, choisissez les liens précédents dans le Guide de référence de l'API de l'Audit Manager. Cela inclut des informations sur l'utilisation de cette opération et de ce paramètre dans l'un des SDK spécifiques au langage AWS .

Ressources supplémentaires

- Pour toutes instructions sur la création de clés, consultez Création de clés dans le AWS Key Management Service Guide de l'utilisateur.
- Pour obtenir des instructions sur la façon d'accorder des autorisations au niveau de la politique clé, voir Autoriser les utilisateurs d'autres comptes à utiliser une clé KMS dans le Guide du AWS Key Management Service développeur.

Ajouter un administrateur délégué

Si vous utilisez AWS Organizations et souhaitez activer le support multi-comptes pour AWS Audit Manager, vous pouvez désigner un compte membre de votre organisation en tant qu'administrateur délégué pour Audit Manager.

Si vous souhaitez utiliser Audit Manager dans plusieurs régions Région AWS, vous devez désigner un compte d'administrateur délégué séparément dans chaque région. Dans vos paramètres Audit Manager, vous devez désigner le même compte d'administrateur délégué dans toutes les régions.

Prérequis

Prenez note des facteurs suivants qui définissent le mode de fonctionnement de l'administrateur délégué dans Audit Manager :

- Votre compte doit être membre d'une organisation.
- Avant de désigner un administrateur délégué, vous devez activer toutes les fonctionnalités de votre organisation. Vous devez également configurer les paramètres du Security Hub de votre organisation. Audit Manager peut ainsi collecter des éléments probants relatifs au Security Hub à partir de vos comptes membres.
- Le compte d'administrateur délégué doit avoir accès à la clé KMS que vous avez fournie lors de la configuration d'Audit Manager.
- Vous ne pouvez pas utiliser votre compte AWS Organizations de gestion en tant qu'administrateur délégué dans Audit Manager.

Procédure

Vous pouvez ajouter un administrateur délégué à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

> **Note**
>
> Une fois que vous avez ajouté un administrateur délégué dans vos paramètres d'Audit Manager, votre compte de gestion ne peut plus créer d'évaluations supplémentaires dans Audit Manager. En outre, la collecte d'éléments probants s'arrête pour toutes les évaluations existantes créées par le compte de gestion. Audit Manager collecte et joint des éléments probants au compte de l'administrateur délégué, qui est le principal responsable de la gestion des évaluations de votre organisation.

Audit Manager console

Pour ajouter un administrateur délégué sur la console Audit Manager

1. Dans l'onglet Paramètres généraux, accédez à la section Administrateur délégué.
2. Sous ID du compte d'administrateur délégué, entrez l'ID du compte de l'administrateur délégué.
3. Sélectionnez Déléguer.

AWS CLI

Pour ajouter un administrateur délégué dans AWS CLI

Exécutez la register-organization-admin-accountcommande et utilisez le `--admin-account-id` paramètre pour spécifier l'ID de compte de l'administrateur délégué.

Dans l'exemple suivant, remplacez le *texte de l'espace réservé* par vos propres informations.

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

Pour ajouter un administrateur délégué à l'aide de l'API

Appelez l'RegisterOrganizationAdminAccountopération et utilisez le adminAccountIdparamètre pour spécifier l'ID de compte de l'administrateur délégué.

Pour plus d'informations, choisissez les liens précédents dans le Guide de référence de l'API de l'Audit Manager. Cela inclut des informations sur l'utilisation de cette opération et de ce paramètre dans l'un des SDK spécifiques au langage AWS .

Étapes suivantes

Pour modifier votre compte d'administrateur délégué, consultezModification d'un administrateur délégué.

Pour supprimer votre compte d'administrateur délégué, consultezSupprimer un administrateur délégué.

Ressources supplémentaires

- Création et gestion d'une organisation
- Résolution des problèmes liés aux administrateurs délégués et à AWS Organizations

Modification d'un administrateur délégué

La modification de votre administrateur délégué AWS Audit Manager est un processus en deux étapes. Tout d'abord, vous devez supprimer le compte administrateur délégué actuel. Vous pouvez ensuite ajouter un nouveau compte en tant qu'administrateur délégué.

Suivez les étapes indiquées sur cette page pour changer d'administrateur délégué.

Table des matières

Prérequis

Avant de supprimer le compte courant

Avant de supprimer le compte d'administrateur délégué actuel, tenez compte des points suivants :

- Tâche de nettoyage de l'outil de recherche de preuves - Si l'administrateur délégué actuel (compte A) a activé l'outil de recherche de preuves, vous devrez effectuer une tâche de nettoyage avant de désigner le compte B comme nouvel administrateur délégué.

  Avant d'utiliser votre compte de gestion pour supprimer le compte A, assurez-vous que le compte A se connecte à Audit Manager et désactive l'outil de recherche de preuves. La désactivation de l'outil de recherche d'éléments probants supprime automatiquement l'entrepôt de données d'événements créé dans le compte lorsque l'outil de recherche d'éléments probants a été activé.

  Si cette tâche n'est pas terminée, le magasin de données d'événements reste dans le compte A. Dans ce cas, nous recommandons à l'administrateur délégué d'origine d'utiliser CloudTrail Lake pour supprimer manuellement le magasin de données d'événements.

  Cette tâche de nettoyage est nécessaire pour éviter de vous retrouver avec plusieurs entrepôts de données d'événements. Audit Manager ignore un entrepôt de données d'événements inutilisé une fois que vous avez supprimé ou modifié un compte d'administrateur délégué. Toutefois, si vous ne supprimez pas le magasin de données d'événements inutilisé, le magasin de données d'événements continue de supporter des frais de stockage de la part de CloudTrail Lake.
- Suppression des données : lorsque vous supprimez un compte d'administrateur délégué pour Audit Manager, les données de ce compte ne sont pas supprimées. Si vous souhaitez supprimer les données de ressources d'un compte d'administrateur délégué, vous devez effectuer cette tâche

séparément avant de supprimer le compte. Vous pouvez également réaliser cette opération dans la console Audit Manager. Vous pouvez également utiliser l'une des opérations d'API de suppression fournies par Audit Manager. Pour obtenir la liste des opérations de suppression disponibles, consultez la section Suppression des données d'Audit Manager.

À l'heure actuelle, Audit Manager ne propose pas d'option permettant de supprimer des éléments probants pour un administrateur délégué spécifique. Au lieu de cela, lorsque votre compte de gestion annule l'enregistrement d'Audit Manager, nous procédons à un nettoyage du compte administrateur délégué actuel au moment de la désinscription.

Avant d'ajouter le nouveau compte

Avant d'ajouter le nouveau compte d'administrateur délégué, tenez compte des points suivants :

- Le nouveau compte doit appartenir à une organisation.
- Avant de désigner un nouvel administrateur délégué, vous devez activer toutes les fonctionnalités de votre organisation. Vous devez également configurer les paramètres du Security Hub de votre organisation. Audit Manager peut ainsi collecter des éléments probants relatifs au Security Hub à partir de vos comptes membres.
- Le compte d'administrateur délégué doit avoir accès à la clé KMS que vous avez fournie lors de la configuration d'Audit Manager.
- Vous ne pouvez pas utiliser votre compte AWS Organizations de gestion en tant qu'administrateur délégué dans Audit Manager.

Procédure

Vous pouvez modifier un administrateur délégué à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

> **Warning**
>
> Lorsque vous modifiez d'administrateur délégué, vous continuez à avoir accès aux éléments probants que vous avez précédemment collectés sous l'ancien compte d'administrateur délégué. Cependant, Audit Manager arrête de collecter et de joindre des éléments probants à l'ancien compte d'administrateur délégué.

Audit Manager console

Pour modifier l'administrateur délégué actuel sur la console Audit Manager

1. (Facultatif) Si l'administrateur délégué actuel (compte A) a activé l'outil de recherche d'éléments probants, effectuez la tâche de nettoyage suivante :

   - Avant de désigner le compte B comme nouvel administrateur délégué, assurez-vous que le compte A se connecte à Audit Manager et désactive l'outil de recherche d'éléments probants.

     La désactivation de l'outil de recherche d'éléments probants supprime automatiquement l'entrepôt de données d'événements créé lorsque le compte A a activé l'outil de recherche d'éléments probants. Si vous n'effectuez pas cette étape, le compte A doit accéder à CloudTrail Lake et supprimer manuellement le magasin de données d'événements. Dans le cas contraire, le magasin de données événementielles reste dans le compte A et continue de supporter les frais de stockage de CloudTrail Lake.
2. Dans l'onglet Paramètres généraux, accédez à la section Administrateur délégué et choisissez Supprimer.
3. Dans la fenêtre contextuelle qui s'affiche, choisissez Supprimer pour confirmer.
4. Sous ID du compte d'administrateur délégué, entrez l'ID du nouveau compte de l'administrateur délégué.
5. Sélectionnez Déléguer.

AWS CLI

Pour modifier l'administrateur délégué actuel dans AWS CLI

Commencez par exécuter la deregister-organization-admin-accountcommande à l'aide du `--admin-account-id` paramètre pour spécifier l'ID de compte de l'administrateur délégué actuel.

Dans l'exemple suivant, remplacez le *texte de l'espace réservé* par vos propres informations.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Exécutez ensuite la register-organization-admin-accountcommande à l'aide du `--admin-account-id` paramètre pour spécifier l'ID de compte du nouvel administrateur délégué.

Dans l'exemple suivant, remplacez le *texte de l'espace réservé* par vos propres informations.

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

Pour changer l'administrateur délégué actuel à l'aide de l'API

Commencez par appeler l'DeregisterOrganizationAdminAccountopération et utilisez le adminAccountIdparamètre pour spécifier l'ID de compte de l'administrateur délégué actuel.

Appelez ensuite l'RegisterOrganizationAdminAccountopération et utilisez le adminAccountIdparamètre pour spécifier l'ID de compte du nouvel administrateur délégué.

Pour plus d'informations, choisissez les liens précédents dans le Guide de référence de l'API de l'Audit Manager. Cela inclut des informations sur l'utilisation de cette opération et de ce paramètre dans l'un des SDK spécifiques au langage AWS .

Étapes suivantes

Pour supprimer votre compte d'administrateur délégué, consultezSupprimer un administrateur délégué.

Ressources supplémentaires

- Création et gestion d'une organisation
- Résolution des problèmes liés aux administrateurs délégués et à AWS Organizations

Supprimer un administrateur délégué

La suppression du compte d'administrateur délégué met fin à la collecte de preuves supplémentaires pour ce compte, mais vous conservez l'accès aux preuves précédemment collectées.

Si vous devez supprimer votre compte d'administrateur délégué pour Audit Manager, vous pouvez suivre les étapes indiquées sur cette page. Respectez scrupuleusement les conditions préalables et les procédures, car elles impliquent le nettoyage des ressources afin d'éviter des coûts de stockage inutiles.

Prérequis

Avant de supprimer le compte d'administrateur délégué d'Audit Manager, tenez compte des points suivants :

Tâche de nettoyage de la recherche d'éléments probants

Si l'administrateur délégué actuel a activé l'outil de recherche de preuves, vous devez effectuer une tâche de nettoyage.

Avant d'utiliser votre compte de gestion pour supprimer l'administrateur délégué actuel, assurez-vous que le compte administrateur délégué actuel se connecte à Audit Manager et désactive l'outil de recherche de preuves. La désactivation de l'outil de recherche d'éléments probants supprime automatiquement l'entrepôt de données d'événements créé dans le compte lorsque l'outil de recherche d'éléments probants a été activé.

Si cette tâche n'est pas terminée, l'entrepôt de données d'événements reste dans leur compte. Dans ce cas, nous recommandons à l'administrateur délégué d'origine d'utiliser CloudTrail Lake pour supprimer manuellement le magasin de données d'événements.

Cette tâche de nettoyage est nécessaire pour éviter de vous retrouver avec plusieurs entrepôts de données d'événements. Audit Manager ignore un entrepôt de données d'événements inutilisé une fois que vous avez supprimé ou modifié un compte d'administrateur délégué. Toutefois, si vous ne supprimez pas le magasin de données d'événements inutilisé, le magasin de données d'événements continue de supporter des frais de stockage de la part de CloudTrail Lake.

Suppression de données

Lorsque vous supprimez un compte d'administrateur délégué pour Audit Manager, les données de ce compte ne sont pas supprimées. Si vous souhaitez supprimer les données de ressources d'un compte d'administrateur délégué, vous devez effectuer cette tâche séparément avant de supprimer le compte. Vous pouvez également réaliser cette opération dans la console Audit Manager. Vous pouvez également utiliser l'une des opérations d'API de suppression fournies par Audit Manager. Pour obtenir la liste des opérations de suppression disponibles, consultez la section Suppression des données d'Audit Manager.

À l'heure actuelle, Audit Manager ne propose pas d'option permettant de supprimer des éléments probants pour un administrateur délégué spécifique. Au lieu de cela, lorsque votre compte de gestion annule l'enregistrement d'Audit Manager, nous procédons à un nettoyage du compte administrateur délégué actuel au moment de la désinscription.

Procédure

Vous pouvez supprimer un administrateur délégué à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

> **Warning**
>
> Lorsque vous supprimez un administrateur délégué, vous continuez à avoir accès aux éléments probants que vous avez précédemment collectés sous ce compte d'administrateur délégué. Cependant, Audit Manager arrête de collecter et de joindre des éléments probants à l'ancien compte d'administrateur délégué.

Audit Manager console

Pour supprimer l'administrateur délégué actuel sur la console Audit Manager

1. (Facultatif) Si l'administrateur délégué actuel a activé l'outil de recherche d'éléments probants, effectuez la tâche de nettoyage suivante :

   - Assurez-vous que le compte administrateur délégué actuel se connecte à Audit Manager et désactive l'outil de recherche d'éléments probants.

     La désactivation de l'outil de recherche d'éléments probants supprime automatiquement l'entrepôt de données d'événements créé dans le compte lorsque l'outil de recherche d'éléments probants a été activé. Si cette étape n'est pas terminée, le compte d'administrateur délégué doit utiliser CloudTrail Lake pour supprimer manuellement le magasin de données d'événements. Dans le cas contraire, le magasin de données sur les événements reste sur leur compte et continue de supporter les frais de stockage de CloudTrail Lake.
2. Dans l'onglet Paramètres généraux, accédez à la section Administrateur délégué et choisissez Supprimer.
3. Dans la fenêtre contextuelle qui s'affiche, choisissez Supprimer pour confirmer.

AWS CLI

La désactivation de l'outil de recherche d'éléments probants supprime automatiquement l'entrepôt de données d'événements créé dans le compte lorsque l'outil de recherche d'éléments probants a été activé. Si cette étape n'est pas terminée, le compte d'administrateur délégué doit utiliser CloudTrail Lake pour supprimer manuellement le magasin de données d'événements. Dans le cas contraire, le magasin de données sur les événements reste sur leur compte et continue de supporter les frais de stockage de CloudTrail Lake.

Pour supprimer l'administrateur délégué actuel dans AWS CLI

Exécutez la deregister-organization-admin-accountcommande et utilisez le `--admin-account-id` paramètre pour spécifier l'ID de compte de l'administrateur délégué.

Dans l'exemple suivant, remplacez le *`texte de l'espace réservé`* par vos propres informations.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Audit Manager API

Pour supprimer l'administrateur délégué actuel à l'aide de l'API

Appelez l'DeregisterOrganizationAdminAccountopération et utilisez le adminAccountIdparamètre pour spécifier l'ID de compte de l'administrateur délégué.

Pour plus d'informations, choisissez les liens précédents dans le Guide de référence de l'API de l'Audit Manager. Cela inclut des informations sur l'utilisation de cette opération et de ce paramètre dans l'un des SDK spécifiques au langage AWS .

Ressources supplémentaires

- Résolution des problèmes liés aux administrateurs délégués et à AWS Organizations

Configuration de vos propriétaires d'audit par défaut

Vous pouvez utiliser ce paramètre pour spécifier les personnes par défaut audit owner qui ont un accès principal à vos évaluations dans Audit Manager.

Procédure

Vous pouvez mettre à jour ce paramètre à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

Audit Manager console

Vous pouvez choisir parmi les options Comptes AWS répertoriées dans le tableau ou utiliser la barre de recherche pour en rechercher d'autres Comptes AWS.

Pour mettre à jour les responsables de vos audits par défaut sur la console Audit Manager

1. Dans l'onglet Paramètres d'évaluation, accédez à la section Responsables d'audit par défaut et choisissez Modifier.
2. Pour ajouter un responsable d'audit par défaut, sélectionnez la case à cocher en regard du nom du compte sous Responsable de l'audit.
3. Pour supprimer un responsable d'audit par défaut, videz la case à cocher en regard du nom du compte sous Responsable de l'audit.
4. Lorsque vous avez terminé, sélectionnez Enregistrer.

AWS CLI

Pour mettre à jour le responsable de votre audit par défaut dans AWS CLI

Exécutez la commande paramètres de mise à jour et utilisez le paramètre `--default-process-owners` pour préciser un responsable d'audit.

Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations. Notez que `roleType` ne peut être que `PROCESS_OWNER`.

```
aws auditmanager update-settings --default-process-owners
 roleType=PROCESS_OWNER,roleArn=arn:aws:iam::111122223333:role/Administrator
```

Audit Manager API

Pour mettre à jour le responsable de votre audit par défaut à l'aide de l'API

Appelez l'UpdateSettingsopération et utilisez le defaultProcessOwnersparamètre pour spécifier les propriétaires d'audit par défaut. Notez que `roleType` ne peut être que `PROCESS_OWNER`.

Ressources supplémentaires

- Pour plus d'informations sur les responsables d'audit, consultez Responsables d'audit dans la section Concepts et terminologie de ce guide.

Configuration de la destination par défaut de votre rapport d'évaluation

Lorsque vous générez un rapport d'évaluation, Audit Manager publie le rapport dans le compartiment S3 de votre choix. Ce compartiment S3 est appeléassessment report destination. Vous pouvez choisir le compartiment S3 dans lequel Audit Manager stocke vos rapports d'évaluation.

Prérequis

Conseils de configuration pour la destination de votre rapport d'évaluation

Pour garantir la bonne génération de votre rapport d'évaluation, nous vous recommandons d'utiliser les configurations suivantes pour la destination de votre rapport d'évaluation.

Compartiments de la même région

Nous vous recommandons d'utiliser un compartiment S3 qui se trouve dans le même compartiment Région AWS que votre évaluation. Lorsque vous utilisez un compartiment et une évaluation correspondant à la même région, votre rapport d'évaluation peut inclure jusqu'à 22 000 éléments probants. À l'inverse, lorsque vous utilisez un compartiment et une évaluation interrégionaux, seuls 3 500 éléments probants peuvent être inclus.

Région AWS

La Région AWS clé gérée par le client (si vous en avez fourni une) doit correspondre à la région de votre évaluation et au compartiment S3 de destination de votre rapport d'évaluation. Pour obtenir des instructions sur la modification de la clé KMS, reportez-vous àConfiguration de vos paramètres de chiffrement des données. Pour obtenir la liste des régions d'Audit Manager supportées, consultez AWS Audit Manager Points de terminaison et quotas dans Référence générale d'Amazon Web Services.

Chiffrement de compartiment S3

Si la destination de votre rapport d'évaluation dispose d'une politique de compartiment qui nécessite un chiffrement côté serveur (SSE) à l'aide de SSE-KMS, la clé KMS utilisée dans cette politique de compartiment doit correspondre à la clé KMS que vous avez configurée dans les paramètres de chiffrement des données d'Audit Manager. Si vous n'avez pas configuré de clé KMS dans vos paramètres d'Audit Manager et que votre politique de compartiment de destination du rapport d'évaluation nécessite SSE, assurez-vous que la politique de compartiment autorise SSE-S3. Pour obtenir des instructions sur la façon de configurer la clé KMS utilisée pour le chiffrement des données, consultezConfiguration de vos paramètres de chiffrement des données.

Compartiments S3 entre comptes

L'utilisation d'un compartiment S3 multi-comptes comme destination de votre rapport d'évaluation n'est pas prise en charge dans la console Audit Manager. Il est possible de spécifier un bucket multi-comptes comme destination de votre rapport d'évaluation en utilisant le AWS CLI ou l'un des AWS SDK, mais pour des raisons de simplicité, nous vous recommandons de ne pas le faire. Si vous choisissez d'utiliser un compartiment S3 multi-comptes comme destination de votre rapport d'évaluation, tenez compte des points suivants.

- Par défaut, les objets S3, tels que les rapports d'évaluation, appartiennent à Compte AWS celui qui télécharge l'objet. Vous pouvez utiliser le paramètre propriété de l'objet S3 pour modifier ce comportement par défaut afin que tous les nouveaux objets écrits par des comptes avec la liste de contrôle d'accès (ACL) `bucket-owner-full-control` prédéfinie deviennent automatiquement la propriété du propriétaire du compartiment (ACL) prédéfinie.

  Bien que cela ne soit pas obligatoire, nous vous recommandons d'apporter les modifications suivantes aux paramètres de votre compartiment multi-comptes. Ces modifications garantissent que le propriétaire du compartiment a le contrôle total des rapports d'évaluation que vous publiez dans son compartiment.

  - Définissez la propriété de l'objet du compartiment S3 selon les préférences du propriétaire du compartiment, au lieu du rédacteur d'objets par défaut
  - Ajoutez une politique de compartiment pour garantir que les objets chargés dans ce compartiment disposent de l'ACL `bucket-owner-full-control`
- Pour permettre à Audit Manager de publier des rapports dans un compartiment S3 multi-comptes, vous devez ajouter la politique de compartiment S3 suivante à la destination de votre rapport d'évaluation. Remplacez chaque *`espace réservé`* par vos propres informations. L'élément `Principal` de cette politique est l'utilisateur ou le rôle qui possède l'évaluation et

crée le rapport d'évaluation. Le `Resource` précise le compartiment S3 entre comptes dans lequel le rapport est publié.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account assessment report publishing",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
          },
          "Action": [
              "s3:ListBucket",
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetBucketLocation",
              "s3:PutObjectAcl",
              "s3:DeleteObject"
          ],
          "Resource": [
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
          ]
      }
  ]
}
```

Procédure

Vous pouvez mettre à jour ce paramètre à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

Audit Manager console

Pour mettre à jour la destination de votre rapport d'évaluation par défaut sur la console Audit Manager

1. Dans l'onglet Paramètres d'évaluation, accédez à la section Destination du rapport d'évaluation.

2. Pour utiliser un compartiment S3 existant, sélectionnez un nom de compartiment dans le menu déroulant.
3. Pour créer un nouveau compartiment S3, choisissez Create new bucket.
4. Lorsque vous avez terminé, sélectionnez Enregistrer.

AWS CLI

Pour mettre à jour la destination de votre rapport d'évaluation par défaut dans AWS CLI

Exécutez la commande paramètres de mise à jour et utilisez le paramètre `--default-assessment-reports-destination` pour préciser un compartiment S3.

Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations :

```
aws auditmanager update-settings --default-assessment-reports-destination
 destinationType=S3,destination=s3://DOC-EXAMPLE-DESTINATION-BUCKET
```

Audit Manager API

Pour mettre à jour la destination de votre rapport d'évaluation par défaut à l'aide de l'API

Appelez l'UpdateSettingsopération et utilisez le paramètre defaultAssessmentReportsDestination pour spécifier un compartiment S3.

Ressources supplémentaires

- Création d'un bucket
- Rapports d'évaluation

Configuration des notifications de l'Audit Manager

Vous pouvez configurer Audit Manager pour envoyer des notifications à la rubrique Amazon SNS de votre choix. Si vous êtes abonné à cette rubrique SNS, vous recevez des notifications directement chaque fois que vous vous connectez à Audit Manager.

Suivez les étapes décrites sur cette page pour savoir comment consulter et mettre à jour vos paramètres de notification en fonction de vos préférences. Vous pouvez utiliser une rubrique SNS

standard ou une rubrique SNS FIFO (first-in-first-out). Bien qu'Audit Manager prenne en charge l'envoi de notifications aux rubriques FIFO, l'ordre dans lequel les messages sont envoyés n'est pas garanti.

Prérequis

Si vous souhaitez utiliser une rubrique Amazon SNS qui ne vous appartient pas, vous devez configurer votre politique AWS Identity and Access Management (IAM) à cet effet. Plus précisément, vous devez la configurer pour autoriser la publication de la rubrique à partir de l'Amazon Resource Name (ARN). Pour un exemple de politique que vous pouvez utiliser, consultezExemple 1 (Autorisations pour la rubrique SNS).

Procédure

Vous pouvez mettre à jour ce paramètre à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

Audit Manager console

Pour mettre à jour vos paramètres de notification sur la console Audit Manager

1. Dans l'onglet Paramètres d'évaluation, accédez à la section Notifications.
2. Pour utiliser une rubrique SNS existante, sélectionnez son nom dans le menu déroulant.
3. Pour créer une nouvelle rubrique SNS, choisissez Créer une nouvelle rubrique.
4. Lorsque vous avez terminé, sélectionnez Enregistrer.

AWS CLI

Pour mettre à jour vos paramètres de notification dans AWS CLI

Exécutez la commande paramètres de mise à jour et utilisez le paramètre `--sns-topic` pour préciser une rubrique SNS.

Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations :

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-assessment-topic
```

Audit Manager API

Pour mettre à jour vos paramètres de notification à l'aide de l'API

Appelez l'UpdateSettingsopération et utilisez le paramètre SNStopic pour spécifier un sujet SNS.

Ressources supplémentaires

- Pour obtenir des instructions sur la création d'une rubrique Amazon SNS, consultez la section Création d'une rubrique Amazon SNS dans le guide de l'utilisateur Amazon SNS.
- Pour un exemple de politique que vous pouvez utiliser pour autoriser Audit Manager à envoyer des notifications aux rubriques Amazon SNS, voir Exemple 1 (Autorisations pour la rubrique SNS)
- Pour en savoir plus sur la liste des actions qui invoquent des notifications dans Audit Manager, consultezNotifications dans AWS Audit Manager.
- Pour des solutions aux problèmes de notification dans Audit Manager, consultezRésolution des problèmes liés aux notifications.

Activation de l'outil de recherche d'éléments probants

Vous pouvez activer la fonction de recherche de preuves dans Audit Manager pour rechercher des preuves dans votre Compte AWS. Si vous êtes administrateur délégué d'Audit Manager, vous pouvez rechercher des preuves pour tous les comptes membres de votre organisation.

Suivez ces étapes pour savoir comment activer l'outil de recherche de preuves. Portez une attention particulière aux conditions préalables, car vous aurez besoin d'autorisations spécifiques pour créer et gérer un magasin de données d'événements dans CloudTrail Lake pour cette fonctionnalité.

Prérequis

Autorisations requises pour activer l'outil de recherche d'éléments probants

Pour activer Evidence Finder, vous devez disposer des autorisations nécessaires pour créer et gérer un magasin de données sur les événements dans CloudTrail Lake. Pour utiliser cette fonctionnalité, vous devez disposer des autorisations nécessaires pour effectuer des requêtes CloudTrail Lake. Pour un exemple de politique d'autorisation que vous pouvez utiliser, consultezExemple 4 (Autorisations pour activer l'outil de recherche d'éléments probants).

Si vous avez besoin d'aide concernant les autorisations, contactez votre AWS administrateur. Si vous êtes un administrateur AWS , vous pouvez copier la déclaration d'autorisation requise et la joindre à une politique IAM.

Procédure

Demande d'activation de l'outil de recherche d'éléments probants

Vous pouvez effectuer cette tâche à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

> **Note**
>
> Vous devez activer l'outil de recherche de preuves dans chaque Région AWS endroit où vous souhaitez rechercher des preuves.

Audit Manager console

Pour demander l'activation de l'outil de recherche de preuves sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans l'onglet Paramètres de l'outil de recherche d'éléments probants, accédez à la section Recherche d'éléments probants.
3. Choisissez Politique d'autorisation requise, puis View CloudTrail Lake Permissions pour afficher les autorisations requises pour rechercher des preuves. Si vous ne disposez pas encore de ces autorisations, vous pouvez copier cette déclaration de politique et la joindre à une politique IAM.
4. Sélectionnez Activer.
5. Dans la fenêtre contextuelle, choisissez Request to enable.

AWS CLI

Pour demander l'activation de l'outil de recherche de preuves dans AWS CLI

Exécutez la commande update-settings avec le paramètre `--evidence-finder-enabled`.

```
aws auditmanager update-settings --evidence-finder-enabled
```

Audit Manager API

Pour demander l'activation de l'outil de recherche de preuves à l'aide de l'API

Appelez l'UpdateSettingsopération et utilisez le evidenceFinderEnabledparamètre.

Pour plus d'informations, choisissez les liens précédents dans le Guide de référence de l'API de l'Audit Manager. Cela inclut des informations sur l'utilisation de cette opération et de ce paramètre dans l'un des SDK spécifiques au langage AWS .

Étapes suivantes

Après avoir demandé l'activation de l'outil de recherche de preuves, vous pouvez vérifier le statut de votre demande. Pour obtenir des instructions, veuillez consulter Confirmation du statut de chercheur de preuves .

Ressources supplémentaires

- Outil de recherche d'éléments probants
- Résolution des problèmes liés à l'outil de recherche d'éléments probants

Confirmation du statut de chercheur de preuves

Une fois que vous avez soumis votre demande d'activation de l'outil de recherche de preuves, il faut jusqu'à 10 minutes pour activer la fonctionnalité et créer un magasin de données sur les événements. Dès que l'entrepôt de données d'événements est créé, tous les nouveaux éléments probants sont ensuite ingérés dans l'entrepôt de données d'événements.

Lorsque l'outil de recherche d'éléments probants est activé et que l'entrepôt de données sur les événements est créé, nous remplissons le nouvel entrepôt de données sur les événements avec un maximum de deux ans de vos éléments probants passés Ce processus se déroule automatiquement et prend jusqu'à sept jours.

Suivez les étapes indiquées sur cette page pour vérifier et comprendre le statut de votre demande afin d'activer l'outil de recherche de preuves.

Prérequis

Assurez-vous d'avoir suivi les étapes pour activer l'outil de recherche de preuves. Pour obtenir des instructions, veuillez consulter Activation de l'outil de recherche d'éléments probants.

Procédure

Vous pouvez vérifier l'état actuel de l'outil de recherche d'éléments probants à l'aide de la console Audit Manager, de AWS CLI ou de l'API Audit Manager.

Audit Manager console

Pour voir l'état actuel de l'outil de recherche de preuves sur la console Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Sous Activer l'outil de recherche d'éléments probants (facultatif), consultez l'état actuel.

   Chaque état est défini comme suit :

État	Description
L'outil de recherche de preuves n'est pas activé	Vous n'avez pas encore activé l'outil de recherche de preuves avec succès.
Vous avez demandé d'activer l'outil de recherche de preuves	Votre demande est en attente de la création de la banque de données d'événements.
L'outil de recherche de preuves est activé	Le magasin de données d'événements a été créé. Vous pouvez désormais utiliser l'outil de recherche d'éléments probants. En fonction de la quantité d'éléments probants dont vous disposez, il faut jusqu'à sept jours pour remplir le nouvel entrepôt de données d'événements avec vos données d'éléments probants antérieures. Un panneau d'information bleu indique que le remplissage des données est en cours.

État	Description
	Entre-temps, n'hésitez pas à commencer à explorer l'outil de recherche d'éléments probants. Cependant, n'oubliez pas que toutes les données ne sont pas disponibles tant que le remblayage n'est pas terminé.
Vous avez demandé de désactiver l'outil de recherche de preuves	Votre demande est en attente de la suppression de la banque de données d'événements.
L'outil de recherche de preuves a été désactivé	L'outil de recherche de preuves a été définitivement désactivé et le magasin de données des événements a été supprimé.

AWS CLI

Pour connaître l'état actuel de l'outil de recherche de preuves dans le AWS CLI

Exécutez la commande update-settings avec le paramètre `--attribute`défini sur `EVIDENCE_FINDER_ENABLEMENT`.

```
aws auditmanager get-settings --attribute EVIDENCE_FINDER_ENABLEMENT
```

Cela renvoie les informations suivantes :

enablementStatus

Cet attribut indique l'état actuel de l'outil de recherche d'éléments probants.

- `ENABLE_IN_PROGRESS` : vous avez demandé d'activer l'outil de recherche d'éléments probants. Un entrepôt de données sur les événements est en cours de création pour répondre aux requêtes de recherche d'éléments probants.
- `ENABLED` : un entrepôt de données sur les événements a été créé et l'outil de recherche d'éléments probants est activé. Nous vous recommandons d'attendre sept jours jusqu'à ce que l'entrepôt de données sur les événements soit rempli avec vos anciennes données probantes. Vous pouvez utiliser l'outil de recherche d'éléments probants en attendant, mais toutes les données ne sont pas disponibles tant que le remplissage n'est pas terminé.

- `DISABLE_IN_PROGRESS` : vous avez demandé à désactiver l'outil de recherche d'éléments probants, et votre demande est en attente de suppression de l'entrepôt de données des événements.
- `DISABLED` : vous avez définitivement désactivé l'outil de recherche d'éléments probants et l'entrepôt de données de l'événement est supprimé. Vous ne pouvez pas réactiver l'outil de recherche d'éléments probants après ce point.

backfillStatus

Cet attribut indique l'état actuel du remplissage des données d'éléments probants.

- `NOT_STARTED` : le remplissage n'a pas encore commencé.
- `IN_PROGRESS` : le remplissage est en cours. Cela prend jusqu'à sept jours, selon la quantité de données d'éléments probants.
- `COMPLETED` : le remblayage est terminé. Tous vos éléments probants passés sont désormais interrogeables.

Audit Manager API

Pour voir l'état actuel de l'outil de recherche de preuves à l'aide de l'API

Appelez l'GetSettingsopération avec le `attribute` paramètre défini sur`EVIDENCE_FINDER_ENABLEMENT`. Cela renvoie les informations suivantes :

enablementStatus

Cet attribut indique l'état actuel de l'outil de recherche d'éléments probants.

- `ENABLE_IN_PROGRESS` : vous avez demandé d'activer l'outil de recherche d'éléments probants. Un entrepôt de données sur les événements est en cours de création pour répondre aux requêtes de recherche d'éléments probants.
- `ENABLED` : un entrepôt de données sur les événements a été créé et l'outil de recherche d'éléments probants est activé. Nous vous recommandons d'attendre sept jours jusqu'à ce que l'entrepôt de données sur les événements soit rempli avec vos anciennes données probantes. Vous pouvez utiliser l'outil de recherche d'éléments probants en attendant, mais toutes les données ne sont pas disponibles tant que le remplissage n'est pas terminé.

- `DISABLE_IN_PROGRESS` : vous avez demandé à désactiver l'outil de recherche d'éléments probants, et votre demande est en attente de suppression de l'entrepôt de données des événements.
- `DISABLED` : vous avez définitivement désactivé l'outil de recherche d'éléments probants et l'entrepôt de données de l'événement est supprimé. Vous ne pouvez pas réactiver l'outil de recherche d'éléments probants après ce point.

backfillStatus

Cet attribut indique l'état actuel du remplissage des données d'éléments probants.

- `NOT_STARTED` signifie que le remplissage n'a pas encore commencé.
- `IN_PROGRESS` signifie que le remplissage est en cours. Cela prend jusqu'à sept jours, selon la quantité de données d'éléments probants.
- `COMPLETED` signifie que le remplissage est terminé. Tous vos éléments probants passés sont désormais interrogeables.

Pour plus d'informations, consultez evidenceFinderEnablementla référence de l'API Audit Manager.

Étapes suivantes

Une fois que l'outil de recherche de preuves est activé avec succès, vous pouvez commencer à utiliser cette fonctionnalité. Nous vous recommandons d'attendre sept jours jusqu'à ce que l'entrepôt de données sur les événements soit rempli avec vos anciennes données probantes. Vous pouvez utiliser Evidence Finder dans l'intervalle, mais il est possible que toutes les données ne soient pas disponibles tant que le remplissage n'est pas terminé.

Pour commencer à utiliser Evidence Finder, voirRecherche de preuves dans Evidence Finder.

Ressources supplémentaires

- Résolution des problèmes liés à l'outil de recherche d'éléments probants

Désactivation de l'outil de recherche d'éléments probants

Si vous ne souhaitez plus utiliser l'outil de recherche de preuves, vous pouvez désactiver cette fonctionnalité à tout moment.

Suivez ces étapes pour savoir comment désactiver l'outil de recherche de preuves. Portez une attention particulière aux conditions préalables, car vous aurez besoin d'autorisations spécifiques pour supprimer le magasin de données d'événements créé dans CloudTrail Lake lorsque vous avez activé Evidence Finder.

Prérequis

Autorisations requises pour désactiver l'outil de recherche d'éléments probants

Pour désactiver l'outil de recherche de preuves, vous devez être autorisé à supprimer un magasin de données d'événements dans CloudTrail Lake. Pour un exemple de politique que vous pouvez utiliser, consultez Autorisations pour désactiver l'outil de recherche d'éléments probants.

Si vous avez besoin d'aide concernant les autorisations, contactez votre AWS administrateur. Si vous êtes un administrateur AWS , vous pouvez joindre la déclaration d'autorisation requise à une politique IAM.

Procédure

Vous pouvez effectuer cette tâche à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

> **Warning**
>
> La désactivation de l'outil de recherche de preuves supprime le magasin de données d'événements CloudTrail Lake créé par Audit Manager. Par conséquent, vous ne pouvez pas réactiver cette fonctionnalité. Pour réutiliser l'outil de recherche d'éléments probants après l'avoir désactivé, vous devez désactiver AWS Audit Manager puis réactiver complètement le service.

Audit Manager console

Pour désactiver l'outil de recherche de preuves sur la console Audit Manager

1. Dans la section Outil de recherche d'éléments probants de la page des paramètres d'Audit Manager, choisissez Désactiver.

2. Dans la fenêtre contextuelle qui apparaît, entrez **`Yes`** pour confirmer votre décision.
3. Choisissez Demande pour désactiver.

AWS CLI

Pour désactiver l'outil de recherche de preuves dans AWS CLI

Exécutez la commande update-settings avec le paramètre `--no-evidence-finder-enabled`.

```
aws auditmanager update-settings --no-evidence-finder-enabled
```

Audit Manager API

Pour désactiver l'outil de recherche de preuves à l'aide de l'API

Appelez l'UpdateSettingsopération et utilisez le evidenceFinderEnabledparamètre.

Pour plus d'informations, choisissez les liens précédents dans le Guide de référence de l'API de l'Audit Manager. Cela inclut des informations sur l'utilisation de cette opération et de ce paramètre dans l'un des SDK spécifiques au langage AWS .

Ressources supplémentaires

- Résolution des problèmes liés à l'outil de recherche d'éléments probants

Configuration de votre destination d'exportation par défaut pour Evidence Finder

Lorsque vous exécutez des requêtes dans Evidence Finder, vous pouvez exporter les résultats de vos recherches dans un fichier CSV (valeurs séparées par des virgules). Utilisez ce paramètre pour choisir le compartiment S3 par défaut dans lequel Audit Manager enregistre vos fichiers exportés.

Prérequis

Votre compartiment S3 doit disposer de la politique d'autorisation requise pour CloudTrail permettre d'y écrire les fichiers d'exportation. Plus précisément, la politique de compartiment doit inclure une

`s3:PutObject` action et l'ARN du compartiment, et la liste CloudTrail en tant que principal de service.

- Pour un exemple de politique d'autorisation que vous pouvez utiliser, consultezExemple 3 (autorisations de destination d'exportation).
- Pour savoir comment associer cette politique à votre compartiment S3, consultez Ajouter une politique de compartiment à l'aide de la console Amazon S3.
- Pour plus de conseils, consultez les conseils de configuration pour votre destination d'exportation sur cette page.

Conseils de configuration pour votre destination d'exportation

Pour garantir une exportation de fichiers réussie, nous vous recommandons de vérifier les configurations suivantes pour votre destination d'exportation.

Région AWS

La Région AWS clé gérée par le client (si vous en avez fourni une) doit correspondre à la région de votre évaluation. Pour obtenir des instructions sur la modification de la clé KMS, consultez Paramètres du chiffrement des données Audit Manager.

Compartiments S3 entre comptes

L'utilisation d'un compartiment S3 multi-comptes comme destination de votre rapport n'est pas prise en charge dans la console Audit Manager. Il est possible de spécifier un bucket multi-comptes à l'aide du AWS CLI ou de l'un des AWS SDK, mais pour des raisons de simplicité, nous vous recommandons de ne pas le faire. Si vous choisissez d'utiliser un compartiment S3 multi-comptes comme destination de votre export, tenez compte des points suivants.

- Par défaut, les objets S3, tels que les exportations CSV, appartiennent à Compte AWS celui qui télécharge l'objet. Vous pouvez utiliser le paramètre propriété de l'objet S3 pour modifier ce comportement par défaut afin que tous les nouveaux objets écrits par des comptes avec la liste de contrôle d'accès (ACL) `bucket-owner-full-control` prédéfinie deviennent automatiquement la propriété du propriétaire du compartiment (ACL) prédéfinie.

  Bien que cela ne soit pas obligatoire, nous vous recommandons d'apporter les modifications suivantes aux paramètres de votre compartiment multi-comptes. Ces modifications garantissent que le propriétaire du compartiment a le contrôle total des fichiers exportés que vous publiez dans son compartiment.

  - Définissez la propriété de l'objet du compartiment S3 selon les préférences du propriétaire du compartiment, au lieu du rédacteur d'objets par défaut
  - Ajoutez une politique de compartiment pour garantir que les objets chargés dans ce compartiment disposent de l'ACL `bucket-owner-full-control`

- Pour permettre à Audit Manager de publier des rapports dans un compartiment S3 multi-comptes, vous devez ajouter la politique de compartiment S3 suivante au compartiment de destination d'exportation de votre rapport d'évaluation. Remplacez chaque *espace réservé* par vos propres informations. L'élément `Principal` de cette politique est l'utilisateur ou le rôle qui possède l'évaluation et exporte le fichier. Le `Resource` précise le compartiment S3 entre comptes dans lequel le fichier est exporté.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account file exports",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
          },
          "Action": [
              "s3:ListBucket",
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetBucketLocation",
              "s3:PutObjectAcl",
              "s3:DeleteObject"
          ],
          "Resource": [
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
              "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
          ]
      }
  ]
}
```

Procédure

Vous pouvez mettre à jour ce paramètre à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

Audit Manager console

Pour mettre à jour vos paramètres de destination d'exportation sur la console Audit Manager

1. Dans l'onglet Paramètres de l'outil de recherche d'éléments probants, accédez à la section Destination d'exportation.
2. Choisissez l'une des options suivantes :
   - Si vous souhaitez supprimer le compartiment S3 actuel, choisissez Supprimer pour effacer vos paramètres.
   - Si vous souhaitez enregistrer un compartiment S3 par défaut pour la première fois, passez à l'étape 3.
3. Précisez le compartiment S3 dans lequel vous souhaitez stocker vos fichiers exportés.
   - Choisissez Navigateur S3 pour faire votre choix dans la liste de vos compartiments.
   - Vous pouvez également saisir l'URI du compartiment au format suivant : **`s3://bucketname/prefix`**

   > **Tip**
   >
   > Pour que votre compartiment de destination reste organisé, vous pouvez créer un dossier facultatif pour vos exportations CSV. Pour ce faire, ajoutez une barre oblique (**`/`**) et un préfixe à la valeur dans la zone URI de ressource (par exemple, **`/evidenceFinderCSVExports`**). Audit Manager ajoutera alors ce préfixe lors de l'envoi du fichier CSV au compartiment et Amazon S3 génèrera le chemin spécifié par le préfixe. Pour plus d'informations sur les préfixes dans Amazon S3, veuillez consulter Organisation des objets dans la console Amazon S3 dans le Guide de l'utilisateur Amazon Simple Storage Service.
4. Lorsque vous avez terminé, sélectionnez Enregistrer.

Pour plus d'informations sur la façon de créer un compartiment S3, consultez Création d'un compartiment dans le Guide de l'utilisateur Amazon S3.

AWS CLI

Pour mettre à jour vos paramètres de destination d'exportation dans AWS CLI

Exécutez la commande paramètres de mise à jour et utilisez le paramètre `--default-export-destination` pour préciser un compartiment S3.

Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations :

```
aws auditmanager update-settings --default-export-destination
 destinationType=S3,destination=DOC-EXAMPLE-DESTINATION-BUCKET
```

Pour obtenir des instructions sur la création d'un compartiment S3, consultez la section create-bucket dans le manuel AWS CLI Référence de commandes.

Audit Manager API

Pour mettre à jour vos paramètres de destination d'exportation à l'aide de l'API

Appelez l'UpdateSettingsopération et utilisez le defaultExportDestinationparamètre pour spécifier un compartiment S3.

Pour obtenir des instructions sur la création d'un compartiment S3, consultez CreateBucketle manuel Amazon S3 API Reference.

Notifications dans AWS Audit Manager

AWS Audit Manager peut vous informer des actions des utilisateurs via Amazon Simple Notification Service (Amazon SNS).

Audit Manager envoie des notifications quand l'un des événements suivants se produit :

- Le propriétaire de l'audit délègue un ensemble de contrôles à des fins de révision.
- Un délégué soumet un ensemble de contrôles révisé au propriétaire de l'audit.
- Le propriétaire de l'audit effectue la révision d'un ensemble de contrôles.

Ressources supplémentaires

- Pour configurer vos notifications dans Audit Manager, consultezConfiguration des notifications de l'Audit Manager.
- Pour trouver des réponses aux questions et problèmes courants, consultez Résolution des problèmes liés aux notifications la section Dépannage de ce guide.

Résolution des problèmes courants dans AWS Audit Manager

Au cours de votre utilisation AWS Audit Manager, il est possible que vous rencontriez certains problèmes ou défis nécessitant un dépannage. Que vous rencontriez des difficultés liées à la mise en place d'évaluations, à la collecte de preuves ou à tout autre aspect du service, vous pouvez utiliser ce guide de dépannage pour trouver nos recommandations qui vous aideront à résoudre les problèmes courants rapidement et efficacement.

Nous vous encourageons à consulter la liste des sujets ci-dessous, à trouver celui qui correspond le mieux à votre scénario et à suivre les conseils fournis pour vous remettre sur la bonne voie. En suivant les étapes de dépannage fournies, vous pourrez probablement résoudre le problème de manière indépendante et continuer à tirer parti de toutes les fonctionnalités d'Audit Manager. Toutefois, si votre problème spécifique n'est pas traité ici, ou si vous ne parvenez pas à le résoudre après avoir suivi les étapes recommandées, nous vous recommandons de nous contacter AWS Supportpour obtenir de l'aide.

Rubriques

Résolution des problèmes liés aux évaluations et à la collecte d'éléments probants

Vous pouvez utiliser les informations de cette page pour résoudre les problèmes courants d'évaluation et de collecte d'éléments probants dans Audit Manager.

Problèmes liés à la collecte de preuves

Problèmes d'évaluation

J'ai créé une évaluation, mais je ne vois aucun élément probant pour le moment

Si vous ne trouvez aucun élément probant, il est probable que vous n'ayez pas attendu au moins 24 heures après avoir créé l'évaluation ou qu'il y ait une erreur de configuration.

Nous vous recommandons de contrôler les éléments suivants :

1. Assurez-vous que 24 heures se sont écoulées depuis la création de l'évaluation. Les éléments probants automatisés sont disponibles 24 heures après la création de l'évaluation.

2. Assurez-vous que vous utilisez Audit Manager de la même manière Région AWS que Service AWS celle dont vous vous attendez à obtenir des preuves.
3. Si vous vous attendez à recevoir des preuves de contrôle de conformité provenant de AWS Config et AWS Security Hub, assurez-vous que les consoles Security Hub AWS Config et la console Security Hub affichent les résultats de ces contrôles. Les résultats AWS Config et Security Hub doivent s'afficher de la même manière Région AWS que dans laquelle vous utilisez Audit Manager.

Si vous n'observez toujours aucun élément probant dans votre évaluation et que cela n'est pas dû à l'un de ces problèmes, vérifiez les autres causes potentielles décrites sur cette page.

Mon évaluation ne collecte pas de preuves de contrôle de conformité auprès de AWS Security Hub

Si vous ne trouvez aucune preuve attestant d'un AWS Security Hub contrôle de conformité, cela peut être dû à l'un des problèmes suivants.

Configuration manquante dans AWS Security Hub

Ce problème peut être dû au fait que vous ayez manqué certaines étapes de configuration lors de l'activation d' AWS Security Hub.

Pour résoudre ce problème, assurez-vous d'avoir activé Security Hub avec les paramètres requis pour Audit Manager. Pour obtenir des instructions, veuillez consulter Activer et configurer AWS Security Hub (facultatif).

Un nom de contrôle Security Hub n'a pas été saisi correctement dans votre **`ControlMappingSource`**

Lorsque vous utilisez l'API Audit Manager pour créer un contrôle personnalisé, vous pouvez spécifier un contrôle Security Hub en tant que mappage de source de données pour la collecte d'éléments probants. Pour ce faire, vous devez saisir un identifiant de contrôle en tant que `keywordValue`.

Si vous ne trouvez aucun élément probant de vérification de la conformité pour un contrôle Security Hub, il se peut que la `keywordValue` ait été mal saisie dans votre `ControlMappingSource`. La `keywordValue` est sensible à la casse. Si vous ne la saisissez pas correctement, Audit Manager risque de ne pas reconnaître cette règle. Par conséquent,

vous risqueriez de ne pas collecter les éléments probants de vérification de la conformité pour ce contrôle comme prévu.

Pour résoudre ce problème, mettez à jour le contrôle personnalisé et modifiez la `keywordValue`. Le format correct d'un mot clé Security Hub varie. Pour plus de précision, reportez-vous à la liste desContrôles Security Hub pris en charge .

`AuditManagerSecurityHubFindingsReceiver` EventBridge La règle Amazon est manquante

Lorsque vous activez Audit Manager, une règle nommée `AuditManagerSecurityHubFindingsReceiver` est automatiquement créée et activée dans Amazon EventBridge. Cette règle permet à Audit Manager de collecter les résultats de Security Hub à titre d'élément probant.

Si cette règle n'est pas répertoriée et activée dans le Security Hub Région AWS où vous utilisez, Audit Manager ne peut pas collecter les résultats du Security Hub pour cette région.

Pour résoudre ce problème, accédez à la EventBridge console et vérifiez que la `AuditManagerSecurityHubFindingsReceiver` règle existe dans votre Compte AWS. Si la règle n'existe pas, nous vous recommandons de désactiver Audit Manager, puis de réactiver le service. Si cette action ne résout pas le problème, ou s'il n'est pas possible de désactiver Audit Manager, contactez AWS Support pour obtenir de l'aide.

AWS Config Règles liées aux services créées par Security Hub

N'oubliez pas qu'Audit Manager ne collecte pas de preuves à partir des AWS Config règles liées aux services créées par Security Hub. Il s'agit d'un type spécifique de AWS Config règle gérée qui est activé et contrôlé par le service Security Hub. Security Hub crée des instances de ces règles liées aux services dans votre AWS environnement, même si d'autres instances des mêmes règles existent déjà. Par conséquent, pour éviter la duplication des éléments probants, Audit Manager ne prend pas en charge la collecte d'éléments probants en provenance des règles liées aux services.

J'ai désactivé un contrôle de sécurité dans Security Hub. L'Audit Manager collecte-t-il des preuves de contrôle de conformité pour ce contrôle de sécurité ?

Audit Manager ne collecte pas de preuves concernant les contrôles de sécurité désactivés.

Si vous définissez le statut d'un contrôle de sécurité sur désactivé dans Security Hub, aucun contrôle de sécurité n'est effectué pour ce contrôle dans le compte actuel et dans la région. Par conséquent,

aucun résultat de sécurité n'est disponible dans Security Hub, et aucune preuve connexe n'est collectée par Audit Manager.

En respectant le statut de désactivation que vous avez défini dans Security Hub, Audit Manager garantit que votre évaluation reflète avec précision les contrôles de sécurité actifs et les résultats pertinents pour votre environnement, à l'exclusion des contrôles que vous avez intentionnellement désactivés.

J'ai défini le statut d'une découverte sur « **`Suppressed`** dans Security Hub ». L'Audit Manager collecte-t-il des preuves de conformité relatives à cette constatation ?

Audit Manager collecte des preuves pour les contrôles de sécurité qui ont supprimé les résultats.

Si vous définissez le statut du flux de travail d'un résultat sur « supprimé » dans Security Hub, cela signifie que vous avez examiné le résultat et que vous pensez qu'aucune action n'est nécessaire. Dans Audit Manager, ces résultats supprimés sont collectés sous forme de preuves et joints à votre évaluation. Les détails des preuves indiquent le statut de l'évaluation `SUPPRESSED` signalée directement par Security Hub.

Cette approche garantit que votre évaluation d'Audit Manager représente fidèlement les résultats de Security Hub, tout en offrant une visibilité sur les résultats supprimés qui pourraient nécessiter un examen ou une prise en compte plus approfondis dans le cadre d'un audit.

Mon évaluation ne collecte pas de preuves de contrôle de conformité auprès de AWS Config

Si vous ne trouvez aucune preuve de vérification de conformité pour une AWS Config règle, cela peut être dû à l'un des problèmes suivants.

L'identifiant de règle n'a pas été saisi correctement dans votre **`ControlMappingSource`**

> Lorsque vous utilisez l'API Audit Manager pour créer un contrôle personnalisé, vous pouvez spécifier une AWS Config règle en tant que mappage des sources de données pour la collecte de preuves. La `keywordValue` que vous spécifiez dépend du type de règle.
>
> Si vous ne voyez aucune preuve de vérification de conformité pour une AWS Config règle, il se peut qu'elle `keywordValue` ait été saisie incorrectement dans votre`ControlMappingSource`. La `keywordValue` est sensible à la casse. Si vous ne la saisissez pas correctement,

Audit Manager risque de ne pas reconnaître la règle. Par conséquent, vous risqueriez de ne pas collecter les éléments probants de vérification de la conformité pour cette règle comme prévu.

Pour résoudre ce problème, mettez à jour le contrôle personnalisé et modifiez la `keywordValue`.

- Pour les règles personnalisées, assurez-vous que la `keywordValue` présente le préfixe `Custom_` suivi du nom de la règle personnalisée. Le format du nom de règle personnalisée peut varier. Pour plus de précision, consultez la console AWS Config pour vérifier les noms de vos règles personnalisées.
- Pour les règles gérées, assurez-vous que la `keywordValue` soit l'identifiant de la règle en `ALL_CAPS_WITH_UNDERSCORES`. Par exemple, `CLOUDWATCH_LOG_GROUP_ENCRYPTED`. Pour plus de précision, consultez la liste des mots clés de règles gérées pris en charge.

> **Note**
>
> Pour certaines règles gérées, l'identifiant de la règle est différent du nom de la règle. Par exemple, l'identifiant de la règle pour restricted-ssh est `INCOMING_SSH_DISABLED`. Assurez-vous d'utiliser l'identifiant de la règle, et non le nom de la règle. Pour trouver un identifiant de règle, choisissez une règle dans la liste des règles gérées et recherchez sa valeur Identifiant.

La règle est une règle AWS Config liée à un service

Vous pouvez utiliser des règles gérées et des règles personnalisées en tant que mappage de source de données pour la collecte d'éléments probants. Cependant, Audit Manager ne collecte pas d'éléments probants en provenance de la plupart des règles liées aux services.

Il n'existe que deux types de règles liées aux services à partir desquels Audit Manager peut collecter des éléments probants :

- Règles liées aux services issues des packs de conformité
- Règles liées aux services provenant de AWS Organizations

Audit Manager ne collecte pas d'éléments probants à partir d'autres règles liées aux services, en particulier des règles comportant un Amazon Resource Name (ARN) contenant le préfixe suivant : `arn:aws:config:*:*:config-rule/aws-service-rule/...`

Audit Manager ne collecte pas d'éléments probants dans le cadre de la plupart des règles AWS Config liées aux services afin d'éviter la duplication des éléments probants dans vos évaluations. Une règle liée à un service est un type spécifique de règle gérée qui permet Services AWS à

d'autres utilisateurs de créer des AWS Config règles dans votre compte. Par exemple, certains contrôles Security Hub utilisent une règle AWS Config liée à un service pour exécuter des contrôles de sécurité. Pour chaque contrôle Security Hub qui utilise une AWS Config règle liée à un service, Security Hub crée une instance de la AWS Config règle requise dans votre AWS environnement. Cela se produit même si la règle d'origine existe déjà dans votre compte. Par conséquent, pour éviter de collecter deux fois les mêmes éléments probants à partir de la même règle, Audit Manager ignore la règle liée au service et ne collecte aucun élément probant à partir de celle-ci.

AWS Config n'est pas activé

AWS Config doit être activé dans votre Compte AWS. Une fois cette configuration effectuée AWS Config , Audit Manager collecte des preuves à chaque fois que l'évaluation d'une AWS Config règle a lieu. Assurez-vous d'avoir activé AWS Config dans votre Compte AWS. Pour obtenir des instructions, voir Activer et configurer AWS Config.

La AWS Config règle évaluait une configuration de ressources avant que vous ne configuriez votre évaluation.

Si votre AWS Config règle est configurée pour évaluer les modifications de configuration d'une ressource spécifique, il se peut que vous constatiez un décalage entre l'évaluation AWS Config et les preuves dans Audit Manager. Cela se produit si l'évaluation des règles a eu lieu avant que vous ne configuriez le contrôle dans votre évaluation Audit Manager. Dans ce cas, Audit Manager ne génère d'éléments probants que lorsque la ressource sous-jacente change à nouveau de statut et déclenche une réévaluation de la règle.

Pour contourner le problème, vous pouvez accéder à la règle dans la AWS Config console et la réévaluer manuellement. Cela implique une nouvelle évaluation de toutes les ressources relatives à cette règle.

Mon évaluation ne collecte pas d'éléments probants de l'activité des utilisateurs auprès d' AWS CloudTrail

Lorsque vous utilisez l'API Audit Manager pour créer un contrôle personnalisé, vous pouvez spécifier un nom d' CloudTrail événement en tant que mappage de source de données pour la collecte de preuves. Pour ce faire, vous devez saisir le nom de l'événement en tant que `keywordValue`.

Si vous ne voyez aucune preuve de l'activité des utilisateurs concernant un CloudTrail événement, il se peut que le fichier `keywordValue` ait été mal saisi dans votre`ControlMappingSource`. La

`keywordValue` est sensible à la casse. Si vous ne la saisissez pas correctement, Audit Manager risque de ne pas reconnaître le nom de l'événement. Par conséquent, vous risqueriez de ne pas collecter les éléments probants de l'activité des utilisateurs pour cet événement comme prévu.

Pour résoudre ce problème, mettez à jour le contrôle personnalisé et modifiez la `keywordValue`. Assurez-vous que l'événement est écrit sous la forme `serviceprefix_ActionName`. Par exemple, `cloudtrail_StartLogging`. Pour plus de précision, vérifiez le préfixe Service AWS et les noms des actions dans la Référence de l'autorisation de service.

Mon évaluation ne collecte pas de preuves de données de configuration pour un appel d' AWS API

Lorsque vous utilisez l'API Audit Manager pour créer un contrôle personnalisé, vous pouvez spécifier un appel d' AWS API en tant que mappage de source de données pour la collecte de preuves. Pour ce faire, vous devez saisir l'appel d'API en tant que `keywordValue`.

Si vous ne voyez aucune preuve de données de configuration pour un appel d' AWS API, il se peut que les données aient `keywordValue` été saisies incorrectement dans votre`ControlMappingSource`. La `keywordValue` est sensible à la casse. Si vous ne la saisissez pas correctement, Audit Manager risque de ne pas reconnaître l'appel d'API. Par conséquent, vous risqueriez de ne pas collecter les éléments probants des données de configuration pour cet appel d'API comme prévu.

Pour résoudre ce problème, mettez à jour le contrôle personnalisé et modifiez la `keywordValue`. Assurez-vous que l'appel d'API est écrit sous la forme `serviceprefix_ActionName`. Par exemple, `iam_ListGroups`. Pour plus de précision, reportez-vous à la liste desAWS Appels d'API pris en charge par AWS Audit Manager.

Un contrôle commun ne collecte aucune preuve automatisée

Lorsque vous passez en revue un contrôle commun, le message suivant peut s'afficher : Ce contrôle commun ne collecte pas de preuves automatisées à partir des contrôles principaux.

Cela signifie qu'aucune source de preuves AWS gérée ne peut actuellement étayer ce contrôle commun. Par conséquent, l'onglet Sources de preuves est vide et aucun contrôle de base n'est affiché.

Lorsqu'un contrôle commun ne collecte pas de preuves automatisées, on parle de contrôle commun manuel. Les contrôles manuels courants nécessitent généralement la fourniture d'enregistrements

physiques et de signatures, ou de détails sur des événements qui se produisent en dehors de votre AWS environnement. Pour cette raison, il n'existe souvent aucune source de AWS données pouvant fournir des preuves à l'appui des exigences du contrôle.

Si un contrôle courant est manuel, vous pouvez toujours l'utiliser comme source de preuves pour un contrôle personnalisé. La seule différence est que le contrôle commun ne collectera aucune preuve automatiquement. Au lieu de cela, vous devrez télécharger manuellement vos propres preuves pour étayer les exigences du contrôle commun.

Pour ajouter des preuves à un contrôle commun manuel

1. Création d'un contrôle personnalisé
   - Suivez les étapes pour créer ou modifier un contrôle personnalisé.
   - Lorsque vous spécifiez les sources de preuves à l'étape 2, choisissez le contrôle commun manuel comme source de preuves.
2. Création d'un cadre personnalisé
   - Suivez les étapes pour créer ou modifier un cadre personnalisé.
   - Lorsque vous spécifiez un ensemble de contrôles à l'étape 2, incluez votre nouveau contrôle personnalisé.
3. Création d'une évaluation
   - Suivez les étapes pour créer une évaluation à partir de votre framework personnalisé.
   - À ce stade, le contrôle commun manuel est désormais une source de preuves dans le cadre d'un contrôle d'évaluation actif.
4. Télécharger des preuves manuelles
   - Suivez les étapes pour ajouter des preuves manuelles au contrôle dans votre évaluation.

> **Note**
>
> À mesure que de nouvelles sources de AWS données seront disponibles à l'avenir, il est possible de mettre à jour le contrôle commun pour inclure les contrôles de base en tant que sources de preuves. AWS Dans ce cas, si le contrôle commun est une source de preuves dans un ou plusieurs de vos contrôles d'évaluation actifs, vous bénéficierez automatiquement de ces mises à jour. Aucune autre configuration n'est nécessaire de votre part, et vous commencerez à collecter des preuves automatisées à l'appui du contrôle commun.

Mes éléments probants sont générés à différents intervalles et je ne sais pas à quelle fréquence ils sont collectés

Les contrôles des évaluations d'Audit Manager sont mappés à différentes sources de données. Chaque source de données possède une fréquence de collecte d'éléments probants différente. Par conséquent, il n'y a pas de one-size-fits-all réponse quant à la fréquence à laquelle les preuves sont collectées. Certaines sources de données évaluent la conformité, tandis que d'autres ne capturent que le statut des ressources et les données de modification sans détermination de la conformité.

Vous trouverez ci-dessous un résumé des différents types de sources de données et de la fréquence à laquelle elles collectent des éléments probants.

Type de source de données	Description	Fréquence de collecte des éléments probants	Lorsque ce contrôle est actif dans une évaluation
AWS CloudTrail	Suit l'activité d'un utilisateur spécifique.	En continu	Audit Manager filtre vos CloudTrail journaux en fonction du mot clé que vous avez choisi. Les journaux traités sont importés en tant qu'éléments probants de l'activité de l'utilisateur.
AWS Security Hub	Capture un instantané du niveau de sécurité de vos ressources en rapportant les résultats de Security Hub.	Selon le calendrier de vérification de Security Hub (généralement toutes les 12 heures environ)	Audit Manager récupère le résultat de sécurité directement depuis Security Hub. Le résultat est importé en tant qu'élément probant de contrôle de la conformité.
AWS Config	Capture un aperçu de la situation en matière de sécurité	Sur la base des paramètres	Audit Manager récupère l'évaluation des règles directement à partir de AWS Config.

Type de source de données	Description	Fréquence de collecte des éléments probants	Lorsque ce contrôle est actif dans une évaluation
	de vos ressources en rapportant les résultats de AWS Config.	définis dans la AWS Config règle	L'évaluation est importée en tant qu'élément probant de contrôle de la conformité.
AWS Appels d'API	Prend un instantané de la configuration de vos ressources directement via un appel d'API à l'adresse spécifiée Service AWS.	Tous les jours, toutes les semaines ou tous les mois	Audit Manager effectue l'appel d'API en fonction de la fréquence que vous spécifiez. La réponse est importée en tant qu'élément probant des données de configuration.

Quelle que soit la fréquence de collecte des éléments probants, les nouveaux éléments probants sont collectés automatiquement tant que l'évaluation est active. Pour plus d'informations, consultez Fréquence de collecte des éléments probants.

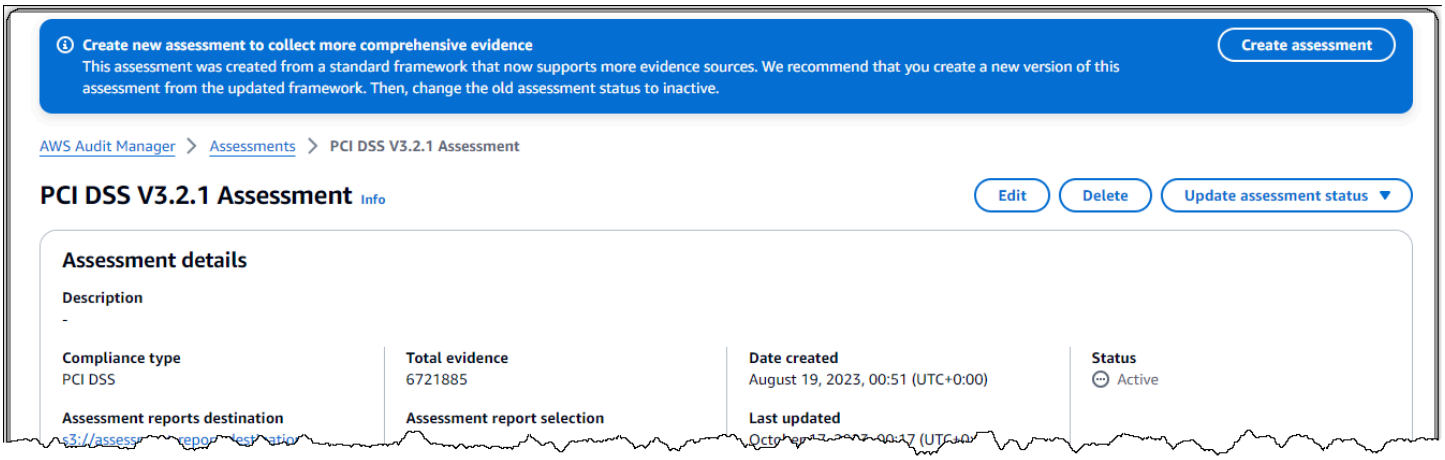
Pour en savoir plus, consultez Types de sources de données pris en charge pour les preuves automatisées et Modifier la fréquence à laquelle un contrôle collecte des preuves.

J'ai désactivé puis réactivé Audit Manager, et à présent, mes évaluations préexistantes ne collectent plus d'éléments probants

Lorsque vous désactivez Audit Manager et que vous choisissez de ne pas supprimer vos données, vos évaluations existantes passent au statut inactif et cessent de collecter des éléments probants. Cela signifie que lorsque vous réactivez Audit Manager, les évaluations que vous avez créées précédemment restent disponibles. Cependant, elles ne reprennent pas automatiquement la collecte d'éléments probants.

Pour qu'une évaluation préexistante recommence à collecter des éléments probants, modifiez l'évaluation et choisissez Enregistrer sans apporter de modifications.

Sur la page des détails de mon évaluation, je suis invité à recréer mon évaluation



Si le message « Créer une nouvelle évaluation pour collecter des preuves plus complètes » s'affiche, cela indique qu'Audit Manager fournit désormais une nouvelle définition du cadre standard à partir duquel votre évaluation a été créée.

Dans la nouvelle définition du cadre, tous les contrôles standard du cadre peuvent désormais collecter des preuves auprès de sources AWS gérées. Cela signifie que chaque fois qu'une mise à jour est apportée aux sources de données sous-jacentes pour un contrôle commun ou principal, Audit Manager applique automatiquement la même mise à jour à tous les contrôles standard associés.

Pour tirer parti de ces sources AWS gérées, nous vous recommandons de créer une nouvelle évaluation à partir du framework mis à jour. Ensuite, vous pouvez modifier l'ancien statut d'évaluation pour le rendre inactif. Cette action permet de garantir que votre nouvelle évaluation recueille les preuves les plus précises et les plus complètes disponibles auprès de sources AWS gérées. Si vous ne prenez aucune mesure, votre évaluation continuera d'utiliser l'ancien cadre et les anciennes définitions de contrôle pour recueillir des preuves exactement comme avant.

Quelle est la différence entre une source de données et une source de preuves ?

Une source de preuves détermine d'où proviennent les preuves. Il peut s'agir d'une source de données individuelle ou d'un groupe prédéfini de sources de données mappé à un contrôle principal ou à un contrôle commun.

Une source de données est le type de source de preuves le plus détaillé. Une source de données inclut les informations suivantes qui indiquent à l'Audit Manager où exactement les données probantes doivent être collectées :

- Type de source de données (par exemple, AWS Config)
- Mappage des sources de données (par exemple, une AWS Config règle spécifique telle que `s3-bucket-public-write-prohibited`)

Mon évaluation n'a pas pu être créée

Si la création de votre évaluation échoue, c'est peut-être parce que vous avez sélectionné un trop grand nombre d' Comptes AWS dans le cadre de votre évaluation. Si vous l'utilisez AWS Organizations, Audit Manager peut prendre en charge jusqu'à 200 comptes membres dans le cadre d'une seule évaluation. Si vous dépassez ce nombre, la création de l'évaluation risque d'échouer. Pour contourner le problème, vous pouvez exécuter plusieurs évaluations avec différents comptes dans le cadre de chaque évaluation.

Que se passe-t-il si je supprime un compte concerné de mon organisation ?

Lorsqu'un compte concerné est supprimé de votre organisation, Audit Manager ne collecte plus d'éléments probants pour ce compte. Cependant, le compte continue d'apparaître dans votre évaluation sous l'onglet Comptes AWS. Pour supprimer le compte de la liste des comptes concernés, modifiez l'évaluation. Le compte supprimé n'apparaît plus dans la liste lors de la modification et vous pouvez enregistrer vos modifications sans que ce compte soit concerné.

Je ne vois pas les services concernés par mon évaluation

Si vous ne voyez pas l'Services AWSonglet, cela signifie que les services concernés sont gérés pour vous par Audit Manager. Lorsque vous créez une nouvelle évaluation, Audit Manager gère les services concernés pour vous à partir de ce moment.

Si vous avez une évaluation plus ancienne, il est possible que vous ayez déjà vu cet onglet dans votre évaluation. Toutefois, Audit Manager supprime automatiquement cet onglet de votre évaluation et prend en charge la gestion des services concernés lorsque l'un des événements suivants se produit :

- Vous modifiez votre évaluation
- Vous modifiez l'un des contrôles personnalisés utilisés dans votre évaluation

Audit Manager déduit les services concernés en examinant vos contrôles d'évaluation et leurs sources de données, puis en mappant ces informations aux informations correspondantes Services AWS. Si une source de données sous-jacente change pour votre évaluation, nous mettons automatiquement à jour le périmètre selon les besoins pour refléter les services appropriés. Cela garantit que votre évaluation recueille des preuves précises et complètes sur tous les services pertinents de votre AWS environnement.

Je ne parviens pas à modifier les services concernés par mon évaluation

Le Modifier une évaluation dans AWS Audit Manager flux de travail ne comporte plus d'étape de services d'édition. Cela est dû au fait qu'Audit Manager gère désormais Services AWS les éléments concernés par votre évaluation.

Si vous avez une évaluation plus ancienne, il est possible que vous ayez défini manuellement les services concernés lors de la création de cette évaluation. Toutefois, vous ne pourrez plus modifier ces services à l'avenir. Audit Manager prend automatiquement en charge la gestion des services concernés par votre évaluation lorsque l'un des événements suivants se produit :

- Vous modifiez votre évaluation
- Vous modifiez l'un des contrôles personnalisés utilisés dans votre évaluation

Audit Manager déduit les services concernés en examinant vos contrôles d'évaluation et leurs sources de données, puis en mappant ces informations aux informations correspondantes Services AWS. Si une source de données sous-jacente change pour votre évaluation, nous mettons automatiquement à jour le périmètre selon les besoins pour refléter les services appropriés. Cela garantit que votre évaluation recueille des preuves précises et complètes sur tous les services pertinents de votre AWS environnement.

Quelle est la différence entre un service concerné et un type de source de données ?

A service in scope est un Service AWS élément inclus dans le champ de votre évaluation. Lorsqu'un service est concerné, Audit Manager collecte des éléments probants concernant votre utilisation de ce service et de ses ressources.

> **Note**
>
> Audit Manager gère Services AWS les domaines concernés par vos évaluations. Si vous avez une évaluation plus ancienne, il est possible que vous ayez spécifié manuellement les services concernés par le passé. À l'avenir, vous ne pourrez ni spécifier ni modifier les services concernés.

Un type de source de données indique d'où proviennent exactement les éléments probants. Si vous chargez vos propres éléments probants, le type de source de données est Manuel. Si Audit Manager collecte les éléments probants, la source de données peut être de quatre types.

1. AWS Security Hub — Capture un aperçu de la situation en matière de sécurité de vos ressources en rapportant les résultats de Security Hub.
2. AWS Config — Capture un aperçu de la situation en matière de sécurité de vos ressources en rapportant les résultats de AWS Config.
3. AWS CloudTrail — Suit l'activité d'un utilisateur spécifique pour une ressource.
4. AWS Appels d'API : prend un instantané de la configuration de vos ressources directement par le biais d'un appel d'API à un utilisateur spécifique Service AWS.

Voici deux exemples illustrant la différence entre un service concerné et le type de source de données.

Exemple 1

Supposons que vous souhaitiez collecter des éléments probants pour un contrôle nommé 4.1.2 - Interdire l'accès en écriture public aux compartiments S3. Ce contrôle vérifie les niveaux d'accès de vos politiques de compartiment S3. Pour ce contrôle, Audit Manager utilise une AWS Config règle spécifique (s3- bucket-public-write-prohibited) pour rechercher une évaluation de vos compartiments S3. Dans cet exemple, les conditions suivantes sont remplies :

- service in scopeC'est Amazon S3
- Les ressources en cours d'évaluation sont vos compartiments S3
- Le type de source de données est AWS Config
- Le mappage des sources de données est une AWS Config règle spécifique (`s3-bucket-public-write-prohibited`)

Exemple 2

Supposons que vous souhaitiez collecter des éléments probants pour un contrôle HIPAA nommé 164.308(a)(5)(ii)(C). Ce contrôle nécessite une procédure de surveillance pour détecter les connexions inappropriées. Pour ce contrôle, Audit Manager utilise des CloudTrail journaux pour rechercher tous les événements de connexion à la console de AWS gestion. Dans cet exemple, les conditions suivantes sont remplies :

- service in scopeC'est IAM
- Les ressources en cours d'évaluation sont vos utilisateurs
- Le type de source de données est CloudTrail
- Le mappage de la source de données est un CloudTrail événement spécifique (`ConsoleLogin`)

Résolution des problèmes liés aux rapports d'évaluation

Vous pouvez utiliser les informations de cette page pour résoudre les problèmes courants liés aux rapports d'évaluation dans Audit Manager.

Rubriques

- Mon rapport d'évaluation n'a pas pu être généré
- J'ai suivi la liste de contrôle ci-dessus et mon rapport d'évaluation n'a toujours pas été généré
- Je reçois un message d'erreur d'accès refusé lorsque j'essaie de générer un rapport
- Je ne suis pas en mesure de décompresser le rapport d'évaluation
- Lorsque je choisis le nom d'un élément probant dans un rapport, je ne suis pas redirigé vers les détails de l'élément probant
- La génération de mon rapport d'évaluation est bloquée au statut En cours, et je ne sais pas quelles répercussions cela aura sur ma facturation
- Ressources supplémentaires

Mon rapport d'évaluation n'a pas pu être généré

Votre rapport d'évaluation n'a peut-être pas été généré pour plusieurs raisons. Vous pouvez commencer à résoudre ce problème en vérifiant les causes les plus fréquentes. Utilisez la liste de contrôle suivante pour commencer.

1. Vérifiez si certaines de vos Région AWS informations ne correspondent pas :
   a. La Région AWS clé gérée par votre client correspond-elle à celle Région AWS de votre évaluation ?

      Si vous avez fourni votre propre clé KMS pour le chiffrement des données d'Audit Manager, la clé doit être Région AWS identique à celle de votre évaluation. Pour résoudre ce problème, remplacez la clé KMS par une clé située dans la même région que votre évaluation. Pour obtenir des instructions sur la modification de la clé KMS, consultezConfiguration de vos paramètres de chiffrement des données.

   b. La Région AWS clé gérée par votre client correspond-elle à celle Région AWS de votre compartiment S3 ?

      Si vous avez fourni votre propre clé KMS pour le chiffrement des données d'Audit Manager, la clé doit se trouver dans le même Région AWS compartiment S3 que vous utilisez comme destination de votre rapport d'évaluation. Pour résoudre ce problème, vous pouvez modifier la clé KMS ou le compartiment S3 afin qu'ils se trouvent tous les deux dans la même région que votre évaluation. Pour obtenir des instructions sur la modification de la clé KMS, consultezConfiguration de vos paramètres de chiffrement des données. Pour obtenir des instructions sur la façon de modifier le compartiment S3, consultezConfiguration de la destination par défaut de votre rapport d'évaluation.

2. Vérifiez les autorisations du compartiment S3 que vous utilisez comme destination du rapport d'évaluation :
   a. L'entité IAM qui génère le rapport d'évaluation possède-t-elle les autorisations nécessaires pour le compartiment S3 ?

      L'entité IAM doit disposer des autorisations nécessaires concernant le compartiment S3 afin de publier des rapports dans ce compartiment. Nous fournissons un exemple de politique que vous pouvez utiliser.

   b. Le compartiment S3 dispose-t-il d'une politique de compartiment qui exige un chiffrement côté serveur (SSE) utilisant SSE-KMS ?

      Si oui, la clé KMS utilisée dans cette politique de compartiment doit correspondre à la clé KMS spécifiée dans vos paramètres de chiffrement des données Audit Manager. Si vous n'avez pas configuré de clé KMS dans vos paramètres Audit Manager et que votre politique de compartiment S3 nécessite SSE, assurez-vous que la politique de compartiment autorise SSE-S3. Pour obtenir des instructions sur la modification de la clé KMS, consultezConfiguration de vos paramètres de chiffrement des données. Pour obtenir des instructions sur la façon

de modifier le compartiment S3, consultezConfiguration de la destination par défaut de votre rapport d'évaluation.

Si vous ne parvenez toujours pas à générer un rapport d'évaluation, passez en revue les problèmes suivants sur cette page.

J'ai suivi la liste de contrôle ci-dessus et mon rapport d'évaluation n'a toujours pas été généré

Audit Manager limite la quantité d'éléments probants que vous pouvez ajouter à un rapport d'évaluation. La limite dépend de votre évaluation, Région AWS de la région du compartiment S3 utilisée comme destination de votre rapport d'évaluation et du fait que votre évaluation utilise ou non un service géré par le client AWS KMS key.

1. La limite est de 22 000 pour les rapports d'une même région (dans le cas où le compartiment S3 et l'évaluation se trouvent dans la même Région AWS)
2. La limite est de 3 500 pour les rapports interrégionaux (dans le cas où le compartiment S3 et l'évaluation se trouvent dans des Régions AWS différentes)
3. La limite est de 3 500 si l'évaluation utilise une clé KMS gérée par le client

Si vous essayez de générer un rapport contenant plus d'éléments probants que les limites susmentionnées, l'opération risque d'échouer.

Pour contourner le problème, vous pouvez générer plusieurs rapports d'évaluation plutôt qu'un seul rapport d'évaluation plus volumineux. Ce faisant, vous pouvez exporter les éléments probants de votre évaluation vers des lots dont la taille est davantage gérable.

Je reçois un message d'erreur d'accès refusé lorsque j'essaie de générer un rapport

Vous recevrez un message d'erreur `access denied` si votre évaluation a été créée par un compte administrateur délégué auquel la clé KMS spécifiée dans vos paramètres Audit Manager n'appartient pas. Pour éviter cette erreur, lorsque vous désignez un administrateur délégué pour Audit Manager, assurez-vous que le compte administrateur délégué a accès à la clé KMS que vous avez fournie lors de la configuration d'Audit Manager.

Vous pouvez également recevoir un message d'erreur `access denied` si vous ne disposez pas des autorisations d'écriture pour le compartiment S3 que vous utilisez comme destination de votre rapport d'évaluation.

Si vous recevez un message d'erreur `access denied`, veillez à respecter les exigences suivantes :

- Votre clé KMS dans vos paramètres Audit Manager donne des autorisations à l'administrateur délégué. Vous pouvez configurer ceci en suivant les instructions de la section Autoriser des utilisateurs d'autres comptes à utiliser une clé KMS dans le Guide du développeur d'AWS Key Management Service . Pour obtenir des instructions sur la façon de vérifier et de modifier vos paramètres de chiffrement dans Audit Manager, consultezConfiguration de vos paramètres de chiffrement des données.
- Vous disposez d'une politique d'autorisation qui vous accorde un accès en écriture au compartiment S3 que vous utilisez comme destination du rapport d'évaluation. Plus précisément, votre politique d'autorisation contient une action `s3:PutObject`, spécifie l'ARN du compartiment S3 et inclut la clé KMS utilisée pour chiffrer vos rapports d'évaluation. Pour un exemple de politique que vous pouvez utiliser, consultezExemple 2 (autorisations de destination du rapport d'évaluation).

> **Note**
>
> Si vous modifiez vos paramètres de chiffrement des données dans Audit Manager, ces modifications s'appliqueront aux nouvelles évaluations que vous créerez à l'avenir. Cela inclut tous les rapports d'évaluation que vous créez à partir de vos nouvelles évaluations.
> Les modifications ne s'appliquent pas aux évaluations existantes que vous avez créées avant de modifier vos paramètres de chiffrement. Cela inclut les nouveaux rapports d'évaluation que vous créez à partir d'évaluations existantes, en plus des rapports d'évaluation existants. Les évaluations existantes, ainsi que tous leurs rapports d'évaluation, continuent d'utiliser l'ancienne clé KMS. Si l'identité IAM qui génère le rapport d'évaluation n'est pas autorisée à utiliser l'ancienne clé KMS, vous pouvez accorder des autorisations au niveau de la stratégie de clé.

Je ne suis pas en mesure de décompresser le rapport d'évaluation

Si vous ne parvenez pas à décompresser le rapport d'évaluation sous Windows, il est probable que Windows Explorer ne puisse pas l'extraire, car son chemin de fichier comporte plusieurs dossiers

imbriqués ou des noms longs. Cela est dû au fait que, dans le système de dénomination des fichiers Windows, le chemin du dossier, le nom du fichier et l'extension du fichier ne peuvent pas dépasser 259 caractères. Dans le cas contraire, cela entraîne un message d'erreur `Destination Path Too Long`.

Pour résoudre ce problème, essayez de déplacer le fichier zip vers le dossier parent de son emplacement actuel. Vous pouvez ensuite réessayer de le décompresser à partir de cet endroit. Vous pouvez également essayer de raccourcir le nom du fichier zip ou de l'extraire vers un autre emplacement dont le chemin de fichier est plus court.

Lorsque je choisis le nom d'un élément probant dans un rapport, je ne suis pas redirigé vers les détails de l'élément probant

Ce problème peut se produire si vous interagissez avec le rapport d'évaluation dans un navigateur ou si vous utilisez le lecteur PDF par défaut installé sur votre système d'exploitation. Certains lecteurs PDF par défaut du navigateur et du système n'autorisent pas l'ouverture de liens relatifs. En d'autres termes, bien que les hyperliens puissent fonctionner dans le résumé PDF du rapport d'évaluation (comme les noms des contrôles liés par des hyperliens dans la table des matières), les hyperliens sont ignorés lorsque vous essayez de quitter le résumé PDF de l'évaluation pour passer à un PDF détaillé des éléments probants distinct.

Si vous rencontrez ce problème, nous vous recommandons d'utiliser un lecteur PDF dédié pour interagir avec vos rapports d'évaluation. Pour une expérience fiable, nous vous recommandons d'installer et d'utiliser Adobe Acrobat Reader, que vous pouvez télécharger sur le site Web d'Adobe. D'autres lecteurs PDF sont également disponibles, mais il a été prouvé qu'Adobe Acrobat Reader fonctionne de manière cohérente et fiable avec les rapports d'évaluation d'Audit Manager.

La génération de mon rapport d'évaluation est bloquée au statut En cours, et je ne sais pas quelles répercussions cela aura sur ma facturation

La génération du rapport d'évaluation n'a aucune répercussion sur la facturation. Vous êtes facturé uniquement en fonction des éléments probants collectés dans le cadre de vos évaluations. Pour plus d'informations sur la tarification, consultez Tarification d'AWS Audit Manager.

Ressources supplémentaires

Les pages suivantes contiennent des conseils pour la résolution des problèmes liés à la génération d'un rapport d'évaluation à partir de l'outil de recherche des éléments probants :

- Je ne parviens pas à générer plusieurs rapports d'évaluation à partir des résultats de ma recherche
- Je ne parviens pas à inclure des éléments probants spécifiques à partir des résultats de ma recherche
- Les résultats de ma recherche d'éléments probants ne sont pas tous inclus dans le rapport d'évaluation
- Je souhaite générer un rapport d'évaluation à partir des résultats de ma recherche, mais mon instruction de requête échoue

Résolution des problèmes liés aux contrôles et aux ensembles de contrôles

Vous pouvez utiliser les informations de cette page pour résoudre les problèmes courants liés aux contrôles dans Audit Manager.

Problèmes généraux

- Je ne vois aucun contrôle ou ensemble de contrôles dans mon évaluation
- Je ne parviens pas à charger des éléments probants manuels dans un contrôle
- Qu'est-ce que cela signifie si une commande indique « Remplacement disponible » ?

Problèmes d'intégration d'AWS Config

- Je dois utiliser plusieurs AWS Config règles comme source de données pour un contrôle unique
- L'option de règle personnalisée n'est pas disponible lorsque je configure une source de données pour un contrôle
- L'option de règle personnalisée est disponible, mais aucune règle n'apparaît dans la liste déroulante
- Certaines règles personnalisées sont disponibles, mais je ne vois pas la règle que je souhaite utiliser
- Je ne vois pas la règle gérée que je souhaite utiliser
- Je souhaite partager un framework personnalisé, mais il comporte des contrôles qui utilisent des AWS Config règles personnalisées comme source de données. Le destinataire peut-il collecter des éléments probants pour ces contrôles ?

- Que se passe-t-il lorsqu'une règle personnalisée est mise à jour dans AWS Config ? Dois-je prendre des mesures dans Audit Manager ?

Je ne vois aucun contrôle ou ensemble de contrôles dans mon évaluation

En bref, pour consulter les contrôles d'une évaluation, vous devez être désigné comme responsable de l'audit de l'évaluation en question. En outre, vous devez disposer des autorisations IAM nécessaires pour consulter et gérer les ressources d'Audit Manager associées.

Si vous avez besoin d'accéder aux contrôles d'une évaluation, demandez à l'un des responsables de l'audit de vous désigner comme responsable de l'audit. Vous pouvez désigner les responsables de l'audit lorsque vous créez ou modifiez une évaluation.

Vérifiez également que vous disposez des autorisations nécessaires pour gérer l'évaluation. Nous recommandons aux responsables de l'audit d'utiliser cette AWSAuditManagerAdministratorAccesspolitique. Si vous avez besoin d'aide concernant les autorisations IAM, contactez votre administrateur ou AWS Support. Pour plus d'informations sur l'attachement d'une politique à une identité IAM, consultez Ajout d'autorisations à un utilisateur et Ajout et suppression d'autorisations basées sur l'identité IAM dans le Guide de l'utilisateur IAM.

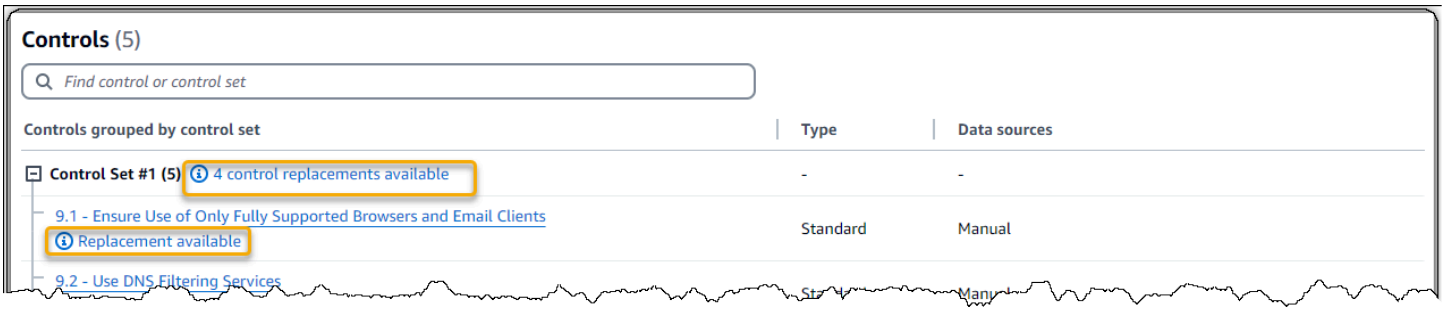
Je ne parviens pas à charger des éléments probants manuels dans un contrôle

Si vous ne pouvez pas charger manuellement des éléments probants dans un contrôle, c'est probablement parce que le statut du contrôle est inactif.

Pour charger des éléments probants manuels dans un contrôle, vous devez d'abord faire passer le statut du contrôle sur En cours de vérification ou Vérifié. Pour obtenir des instructions, veuillez consulter Modification du statut d'un contrôle d'évaluation dans AWS Audit Manager.

> **Important**
>
> Chacun ne Compte AWS peut télécharger manuellement que jusqu'à 100 fichiers de preuves dans un contrôle par jour. Le dépassement de ce quota quotidien entraîne l'échec de tout chargement manuel supplémentaire pour le contrôle en question. Si vous devez charger une grande quantité d'éléments probants manuels dans un seul contrôle, chargez-les par lots sur plusieurs jours.

Qu'est-ce que cela signifie si une commande indique « Remplacement disponible » ?



Si ce message s'affiche, cela signifie qu'une définition de contrôle mise à jour est disponible pour un ou plusieurs contrôles standard de votre framework personnalisé. Nous vous recommandons de remplacer ces contrôles afin de bénéficier des sources de preuves améliorées qu'Audit Manager fournit désormais.

Pour obtenir des instructions sur la procédure à suivre, consultezSur la page de détails de mon framework personnalisé, je suis invité à recréer mon framework personnalisé.

Je dois utiliser plusieurs AWS Config règles comme source de données pour un contrôle unique

Vous pouvez utiliser une combinaison de règles gérées et de règles personnalisées pour un seul contrôle. Pour ce faire, définissez plusieurs sources de preuves pour le contrôle et sélectionnez le type de règle que vous préférez pour chacune d'entre elles. Vous pouvez définir jusqu'à 100 sources de données gérées par le client pour un seul contrôle personnalisé.

L'option de règle personnalisée n'est pas disponible lorsque je configure une source de données pour un contrôle

Cela signifie que vous n'êtes pas autorisé à consulter les règles personnalisées de votre Compte AWS ou de votre organisation. Plus précisément, vous n'êtes pas autorisé à effectuer l'DescribeConfigRulesopération dans la console Audit Manager.

Pour résoudre ce problème, contactez votre AWS administrateur pour obtenir de l'aide. Si vous êtes un administrateur AWS , vous pouvez accorder des autorisations à vos utilisateurs ou à vos groupes en gérant vos politiques IAM.

L'option de règle personnalisée est disponible, mais aucune règle n'apparaît dans la liste déroulante

Cela signifie qu'aucune règle personnalisée n'est activée et ne peut être utilisée dans votre Compte AWS ou dans votre organisation.

Si vous n'avez pas encore de règles personnalisées AWS Config, vous pouvez en créer une. Pour obtenir des instructions, consultez AWS Config custom rules dans le Guide du développeur d'AWS Config .

Si vous vous attendez à voir une règle personnalisée, consultez l'élément de résolution des problèmes suivant.

Certaines règles personnalisées sont disponibles, mais je ne vois pas la règle que je souhaite utiliser

Si vous ne voyez pas la règle personnalisée que vous vous attendez à trouver, cela peut être dû à l'un des problèmes suivants.

Votre compte est exclu de la règle

Il est possible que le compte administrateur délégué que vous utilisez soit exclu de la règle.

Le compte de gestion de votre organisation (ou l'un des comptes d'administrateur AWS Config délégué) peut créer des règles d'organisation personnalisées à l'aide du AWS Command Line Interface (AWS CLI). Lorsque tel est le cas, il peut spécifier une liste de comptes à exclure de la règle. Si votre compte figure dans cette liste, la règle n'est pas disponible dans Audit Manager.

Pour résoudre ce problème, contactez votre AWS Config administrateur pour obtenir de l'aide. Si vous êtes AWS Config administrateur, vous pouvez mettre à jour la liste des comptes exclus en exécutant la put-organization-config-rulecommande.

La règle n'a pas été correctement créée et activée dans AWS Config

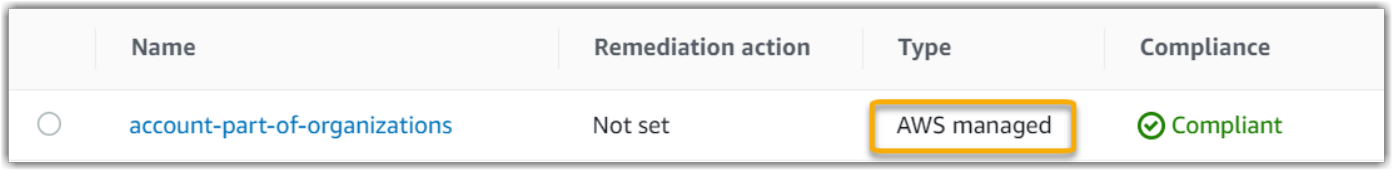
Il est également possible que la règle personnalisée n'ait pas été créée et activée correctement. Si une erreur s'est produite lors de la création de la règle ou si la règle n'est pas activée, elle n'apparaît pas dans la liste des règles disponibles dans Audit Manager.

Pour obtenir de l'aide à ce sujet, nous vous recommandons de contacter votre administrateur AWS Config .

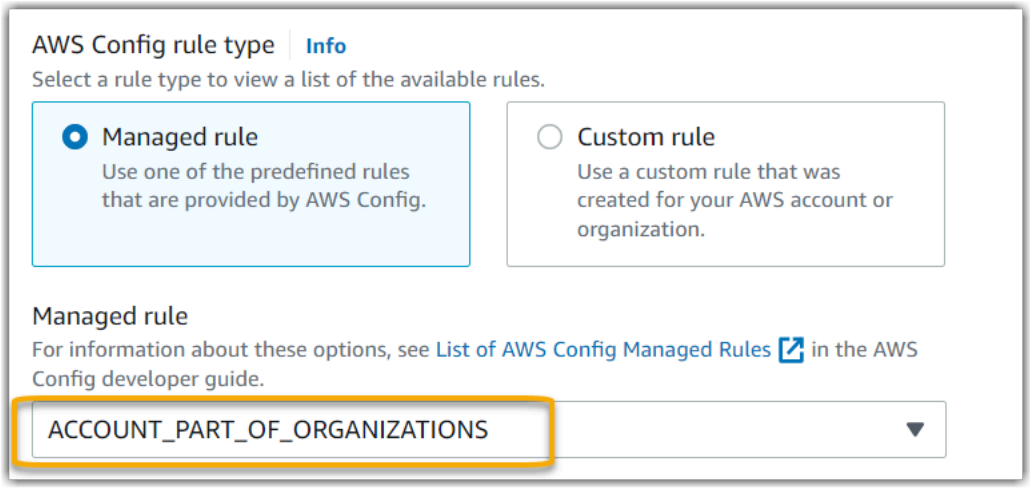
La règle est une règle gérée

Si vous ne trouvez pas la règle que vous recherchez dans la liste déroulante des règles personnalisées, il est possible qu'il s'agisse d'une règle gérée.

Vous pouvez utiliser la console AWS Config pour vérifier si une règle est une règle gérée. Pour ce faire, choisissez Règles dans le menu de navigation de gauche et recherchez la règle dans le tableau. S'il s'agit d'une règle gérée, la colonne Type indique Gérée par AWS .

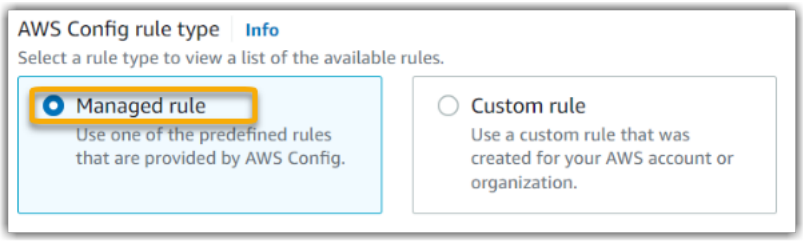


Après avoir vérifié qu'il s'agit d'une règle gérée, revenez dans Audit Manager et sélectionnez Règle gérée comme type de règle. Recherchez ensuite le mot clé identifiant de la règle gérée dans la liste déroulante des règles gérées.



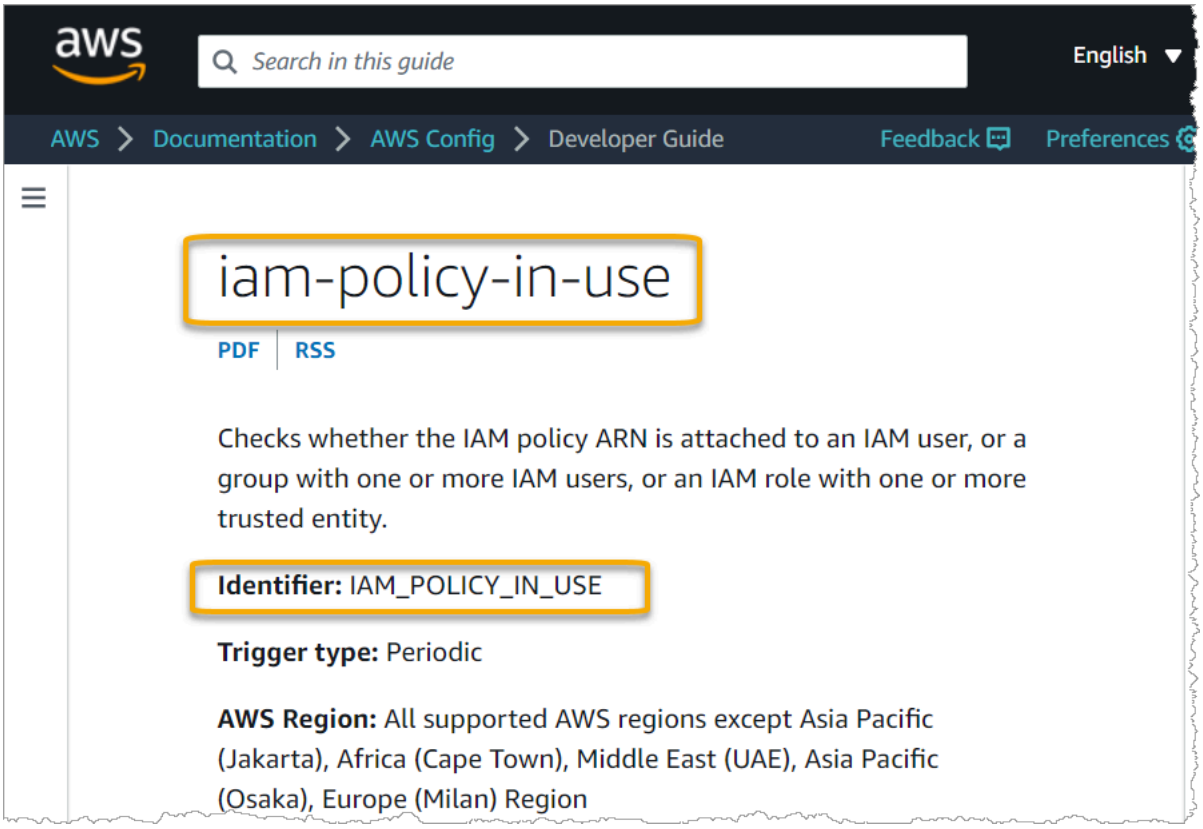
Je ne vois pas la règle gérée que je souhaite utiliser

Avant de sélectionner une règle dans la liste déroulante de la console Audit Manager, assurez-vous d'avoir sélectionné Règle gérée comme type de règle.

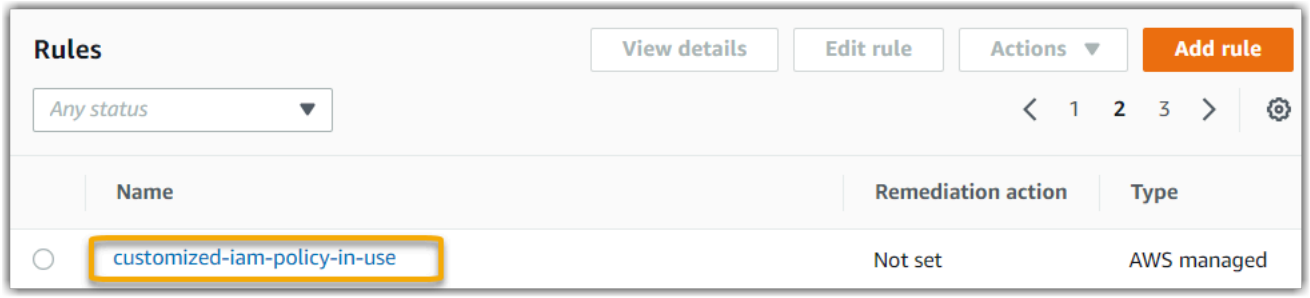


Si vous ne voyez toujours pas la règle gérée que vous vous attendez à trouver, il est possible que vous recherchiez le nom de la règle. Vous devez plutôt rechercher l'identifiant de la règle.

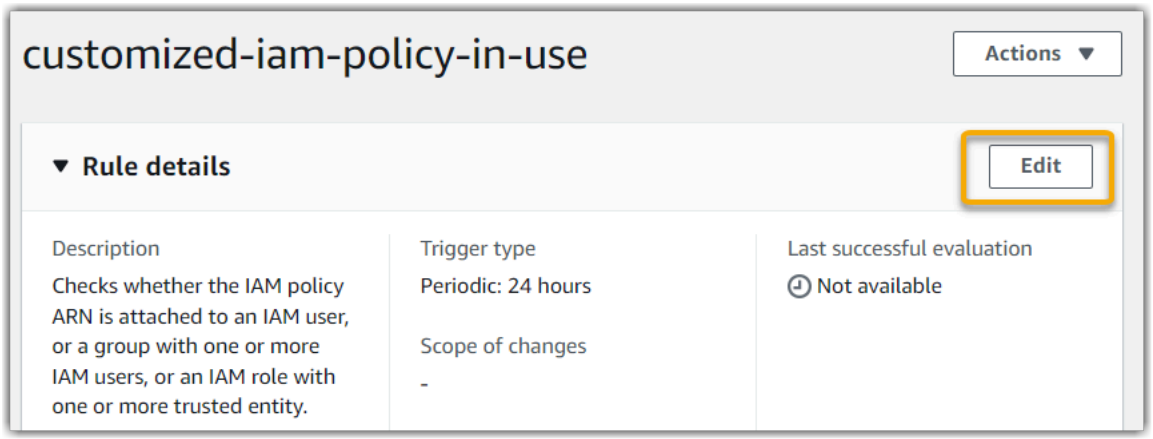
Si vous utilisez une règle gérée par défaut, le nom et l'identifiant sont similaires. Le nom est en minuscules et utilise des tirets (par exemple, `iam-policy-in-use`). L'identifiant est en majuscules et utilise des traits de soulignement (par exemple, `IAM_POLICY_IN_USE`). Pour trouver l'identifiant d'une règle gérée par défaut, consultez la liste des mots clés des règles AWS Config gérées prises en charge et suivez le lien de la règle que vous souhaitez utiliser. Vous accédez ainsi à la AWS Config documentation relative à cette règle gérée. À partir de là, vous pouvez voir à la fois le nom et l'identifiant. Recherchez le mot clé identifiant dans la liste déroulante d'Audit Manager.



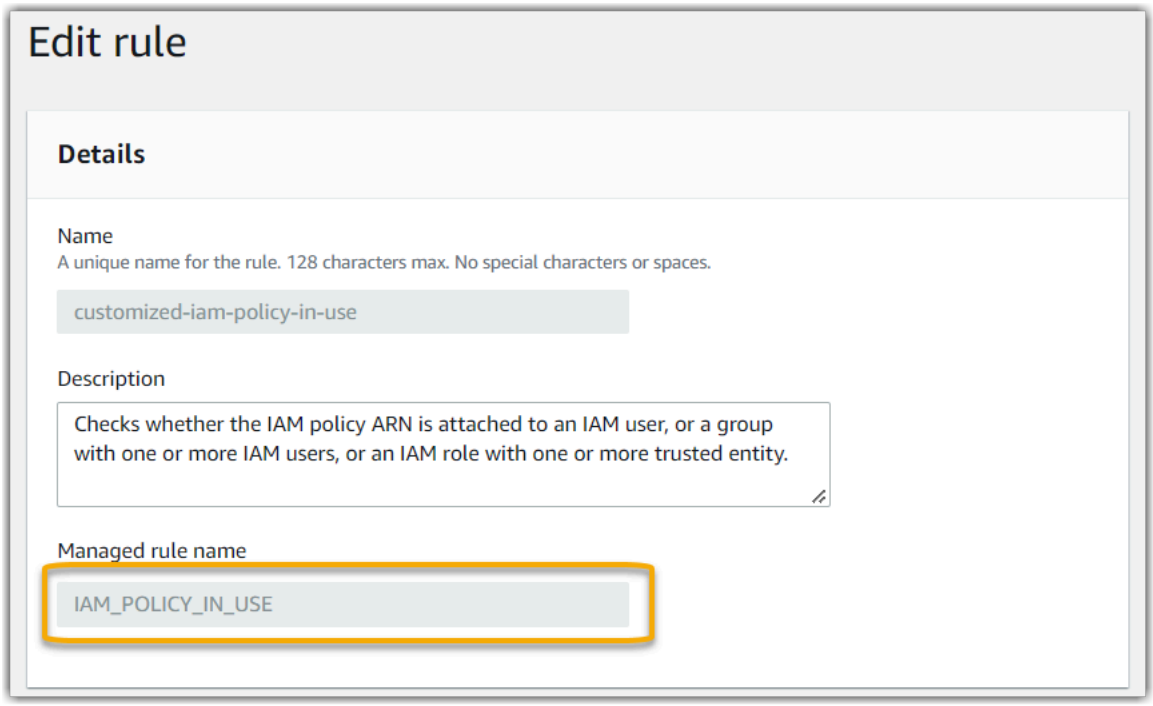
Si vous utilisez une règle gérée personnalisée, vous pouvez utiliser la AWS Config console pour trouver l'identifiant de la règle. Par exemple, supposons que vous souhaitiez utiliser la règle gérée appelée `customized-iam-policy-in-use`. Pour trouver l'identifiant de cette règle, accédez à la AWS Config console, choisissez Règles dans le menu de navigation de gauche, puis choisissez la règle dans le tableau.



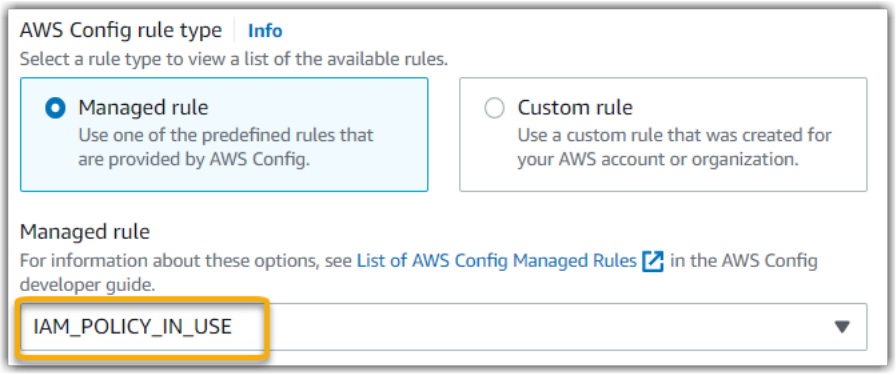
Choisissez Modifier pour afficher les détails de la règle gérée.



Dans la section Détails, vous pouvez trouver l'identifiant source à partir duquel la règle gérée a été créée (`IAM_POLICY_IN_USE`).



Vous pouvez maintenant revenir à la console Audit Manager et sélectionner le même mot clé identifiant dans la liste déroulante.



Je souhaite partager un framework personnalisé, mais il comporte des contrôles qui utilisent des AWS Config règles personnalisées comme source de données. Le destinataire peut-il collecter des éléments probants pour ces contrôles ?

Oui, le destinataire peut collecter des éléments probants pour ces contrôles, mais quelques étapes sont nécessaires pour y parvenir.

Pour qu'Audit Manager collecte des preuves en utilisant une AWS Config règle comme mappage de source de données, les conditions suivantes doivent être vraies. Cela s'applique aux règles gérées et aux règles personnalisées.

1. La règle doit exister dans l' AWS environnement du destinataire
2. La règle doit être activée dans l' AWS environnement du destinataire

N'oubliez pas que les AWS Config règles personnalisées de votre compte n'existent probablement pas déjà dans l' AWS environnement du destinataire. De plus, lorsque le destinataire accepte la demande de partage, Audit Manager ne recrée aucune de vos règles personnalisées dans son compte. Pour que le destinataire puisse collecter des preuves en utilisant vos règles personnalisées comme mappage de sources de données, il doit créer les mêmes règles personnalisées dans son instance de AWS Config. Une fois que le destinataire a créé puis activé les règles, Audit Manager peut collecter des éléments probants à partir de cette source de données.

Nous vous recommandons de communiquer avec le destinataire pour lui faire savoir si des règles personnalisées doivent être créées dans son instance de AWS Config.

Que se passe-t-il lorsqu'une règle personnalisée est mise à jour dans AWS Config ? Dois-je prendre des mesures dans Audit Manager ?

Pour les mises à jour des règles au sein de votre AWS environnement

Si vous mettez à jour une règle personnalisée dans votre AWS environnement, aucune action n'est nécessaire dans Audit Manager. Audit Manager détecte et gère les mises à jour des règles comme décrit dans le tableau suivant. Audit Manager ne vous avertit pas lorsqu'une mise à jour des règles est détectée.

Scénario	Ce que fait Audit Manager	Ce que vous devez faire
Une règle personnalisée est mise à jour dans votre instance de AWS Config	Audit Manager continue de rapporter les résultats relatifs à cette règle à l'aide de la définition de règle mise à jour.	Aucune action n'est nécessaire.
Une règle personnalisée est supprimée dans votre instance de AWS Config	Audit Manager arrête de rapporter les résultats relatifs à la règle supprimée.	Aucune action n'est nécessaire. Si vous le souhaitez, vous pouvez modifier les contrôles personnalisés qui ont utilisé la règle supprimée comme mappage de source de données. Cela permet de nettoyer les paramètres de votre source de données en retirant la règle supprimée. Dans le cas contraire, le nom de la règle supprimée reste un mappage de source de données inutilisé.

Pour les mises à jour des règles en dehors de votre AWS environnement

Si une règle personnalisée est mise à jour en dehors de votre AWS environnement, Audit Manager ne détecte pas la mise à jour de la règle. C'est un élément à prendre en compte si vous utilisez des cadres personnalisés partagés. Cela est dû au fait que, dans ce scénario, l'expéditeur et le destinataire travaillent chacun dans AWS des environnements distincts. Le tableau suivant fournit les actions recommandées pour ce scénario.

Votre rôle	Scénario	Action recommandée
Expédi r	• Vous avez partagé un cadre qui utilise des règles personnalisées comme mappage de source de données. • Après avoir partagé le framework, vous avez mis à jour ou supprimé l'une de ces règles dans AWS Config.	Informez le destinataire de votre mise à jour. Il peut ainsi appliquer la même mise à jour et rester synchronisé avec la dernière définition de règle.
Destina ire	• Vous avez accepté un cadre partagé qui utilise des règles personnalisées comme mappage de source de données. • Après avoir recréé les règles personnal isées dans votre instance de AWS Config, l'expéditeur a mis à jour ou supprimé l'une de ces règles.	Effectuez la mise à jour de la règle correspondante dans votre propre instance de AWS Config.

Résolution des problèmes liés au tableau de bord

Vous pouvez utiliser les informations de cette page pour résoudre les problèmes courants liés au tableau de bord dans Audit Manager.

Rubriques

- L'instantané quotidien affiche des nombres variables d'éléments probants tous les jours. Est-ce normal ?

Mon tableau de bord ne comporte aucune donnée

Si les chiffres du Aperçu quotidien widget sont marqués d'un trait d'union (-), cela indique qu'aucune donnée n'est disponible. Vous devez disposer d'au moins une évaluation active pour voir les données dans le tableau de bord. Pour commencer, créez une évaluation. Après une période de 24 heures, vos données d'évaluation commenceront à apparaître dans le tableau de bord.

> **Note**
>
> Si les chiffres du widget d'instantané quotidien affichent un zéro (0), cela indique que vos évaluations actives (ou l'évaluation que vous avez sélectionnée) ne contiennent aucun élément probant non conforme.

Je ne peux plus voir les données du tableau de bord pour mon évaluation

Audit Manager n'affiche pas les données du tableau de bord pour les évaluations créées à l'aide de l'ancienne version des frameworks standard. Vous pouvez résoudre ce problème en recréant votre évaluation à partir de la dernière version du cadre standard.

Lorsque Audit Manager a lancé la bibliothèque de contrôles communs le 6 juin 2024, nous avons mis à jour tous les frameworks standard. Dans les nouvelles définitions du cadre, tous les contrôles standard du cadre peuvent désormais recueillir des preuves auprès de AWS managed source s. Cela signifie que chaque fois qu'une mise à jour est apportée aux sources de données sous-jacentes pour un contrôle commun ou principal, Audit Manager applique automatiquement la même mise à jour à tous les contrôles standard associés.

Il n'est pas nécessaire de créer une nouvelle évaluation chaque fois que ces mappages de sources de données sont automatiquement mis à jour. La création d'une nouvelle évaluation est une activité ponctuelle que nous vous recommandons d'effectuer après le lancement des contrôles communs.

Pour voir les données d'information sur le tableau de bord à l'avenir, créez une nouvelle évaluation à partir de la version mise à jour du cadre standard. Une fois votre nouvelle évaluation créée, vous pouvez modifier le statut de l'ancienne évaluation pour qu'elle soit inactive.

L'option de téléchargement CSV n'est pas disponible

Cette option est disponible uniquement pour les évaluations individuelles. Assurez-vous d'avoir appliqué un Filtre d'évaluation au tableau de bord, puis réessayez. N'oubliez pas que vous pouvez télécharger un seul fichier CSV à la fois.

Je ne vois pas le fichier téléchargé lorsque j'essaie de télécharger un fichier CSV

Si un domaine de contrôle contient un grand nombre de contrôles, il peut se produire un court délai avant que l'Audit Manager ne génère le fichier CSV. Une fois le fichier généré, celui-ci est automatiquement téléchargé.

Si le fichier téléchargé n'apparaît toujours pas, assurez-vous que votre connexion Internet fonctionne normalement et que vous utilisez la version la plus récente de votre navigateur Web. Vérifiez également votre dossier de téléchargements récents. Les fichiers sont téléchargés dans l'emplacement par défaut déterminé par votre navigateur. Si cela ne résout pas le problème, essayez de télécharger le fichier à l'aide d'un autre navigateur.

Un contrôle ou un domaine de contrôle spécifique est absent du tableau de bord

Cela signifie probablement que vos évaluations actives (ou l'évaluation spécifiée) ne contiennent aucune donnée pertinente pour ce contrôle ou ce domaine de contrôle.

Un domaine de contrôle est affiché sur le tableau de bord uniquement si les deux critères suivants sont remplis :

- Vos évaluations actives (ou l'évaluation spécifiée) contiennent au moins un contrôle lié à ce domaine
- Au moins un contrôle de ce domaine a collecté des éléments probants à la date indiquée en haut du tableau de bord

Un contrôle n'est affiché au sein d'un domaine que s'il a collecté des éléments probants à la date indiquée en haut du tableau de bord.

L'instantané quotidien affiche des nombres variables d'éléments probants tous les jours. Est-ce normal ?

Les éléments probants ne sont pas tous collectés quotidiennement. Les contrôles des évaluations d'Audit Manager sont mappés à différentes sources de données, et chacune d'elles peut avoir un calendrier de collecte d'éléments probants différent. Par conséquent, il est prévu que l'instantané quotidien affiche un nombre variable d'éléments probants tous les jours. Pour plus d'informations, consultez Fréquence de collecte des éléments probants.

Résolution des problèmes liés aux administrateurs délégués et à AWS Organizations

Vous pouvez utiliser les informations de cette page pour résoudre les problèmes courants liés aux administrateurs délégués dans Audit Manager.

Rubriques

Je ne parviens pas à configurer Audit Manager avec mon compte administrateur délégué

Bien que plusieurs administrateurs délégués soient pris en charge AWS Organizations, Audit Manager n'autorise qu'un seul administrateur délégué. Si vous essayez de désigner plusieurs administrateurs délégués dans Audit Manager, vous recevez le message d'erreur suivant :

- Console : `You have exceeded the allowed number of delegated administrators for the delegated service`

- CLI : `An error occurred (ValidationException) when calling the RegisterAccount operation: Cannot change delegated Admin for an active account 11111111111 from 2222222222222 to 333333333333`

Choisissez le compte individuel que vous souhaitez utiliser en tant qu'administrateur délégué dans Audit Manager. Assurez-vous d'abord d'enregistrer le compte administrateur délégué dans Organizations, puis d'ajouter le même compte en tant qu'administrateur délégué dans Audit Manager.

Lorsque je crée une évaluation, je ne parviens pas à voir les comptes de mon organisation sous Comptes concernés

Si vous souhaitez que votre évaluation Audit Manager inclue plusieurs comptes de votre organisation, vous devez spécifier un administrateur délégué.

Vérifiez que vous avez configuré un compte administrateur délégué pour Audit Manager. Pour obtenir des instructions, veuillez consulter Ajouter un administrateur délégué.

Voici quelques points à garder à l'esprit :

- Vous ne pouvez pas utiliser votre compte AWS Organizations de gestion en tant qu'administrateur délégué dans Audit Manager.
- Si vous souhaitez activer Audit Manager dans plusieurs régions Région AWS, vous devez désigner un compte d'administrateur délégué séparément dans chaque région. Dans vos paramètres Audit Manager, désignez le même compte administrateur délégué dans toutes les régions.
- Lorsque vous désignez un administrateur délégué, assurez-vous que le compte administrateur délégué a accès à la clé KMS que vous avez fournie lors de la configuration d'Audit Manager. Pour savoir comment vérifier et modifier vos paramètres de chiffrement, consultezConfiguration de vos paramètres de chiffrement des données.

Je reçois un message d'erreur accès refusé lorsque j'essaie de générer un rapport d'évaluation à l'aide de mon compte administrateur délégué

Vous recevrez un message d'erreur `access denied` si votre évaluation a été créée par un compte administrateur délégué auquel la clé KMS spécifiée dans vos paramètres Audit Manager n'appartient pas. Pour éviter cette erreur, lorsque vous désignez un administrateur délégué pour Audit Manager, assurez-vous que le compte administrateur délégué a accès à la clé KMS que vous avez fournie lors de la configuration d'Audit Manager.

Vous pouvez également recevoir un message d'erreur `access denied` si vous ne disposez pas des autorisations d'écriture pour le compartiment S3 que vous utilisez comme destination de votre rapport d'évaluation.

Si vous recevez un message d'erreur `access denied`, veillez à respecter les exigences suivantes :

- Votre clé KMS dans vos paramètres Audit Manager donne des autorisations à l'administrateur délégué. Vous pouvez configurer ceci en suivant les instructions de la section Autoriser des utilisateurs d'autres comptes à utiliser une clé KMS dans le Guide du développeur d'AWS Key Management Service . Pour obtenir des instructions sur la façon de vérifier et de modifier vos paramètres de chiffrement dans Audit Manager, consultezConfiguration de vos paramètres de chiffrement des données.
- Vous disposez d'une politique d'autorisation qui vous accorde un accès en écriture à la destination du rapport d'évaluation. Plus précisément, votre politique d'autorisation contient une action `s3:PutObject`, spécifie l'ARN du compartiment S3 et inclut la clé KMS utilisée pour chiffrer vos rapports d'évaluation. Pour un exemple de politique que vous pouvez utiliser, consultezExemple 2 (autorisations de destination du rapport d'évaluation).

> **Note**
>
> Si vous modifiez vos paramètres de chiffrement des données dans Audit Manager, ces modifications s'appliqueront aux nouvelles évaluations que vous créerez à l'avenir. Cela inclut tous les rapports d'évaluation que vous créez à partir de vos nouvelles évaluations.
> Les modifications ne s'appliquent pas aux évaluations existantes que vous avez créées avant de modifier vos paramètres de chiffrement. Cela inclut les nouveaux rapports d'évaluation que vous créez à partir d'évaluations existantes, en plus des rapports d'évaluation existants.
> Les évaluations existantes, ainsi que tous leurs rapports d'évaluation, continuent d'utiliser l'ancienne clé KMS. Si l'identité IAM qui génère le rapport d'évaluation n'est pas autorisée à utiliser l'ancienne clé KMS, vous pouvez accorder des autorisations au niveau de la stratégie de clé.

Que se passe-t-il dans Audit Manager si je dissocie un compte membre de mon organisation ?

Lorsque vous dissociez un compte membre d'une organisation, Audit Manager reçoit une notification concernant cet événement. Audit Manager supprime ensuite automatiquement cet Compte AWS

des listes des comptes concernés par vos évaluations existantes. Lorsque vous définissez l'étendue des nouvelles évaluations à venir, le compte dissocié n'apparaît plus dans la liste des Comptes AWSéligibles.

Lorsqu'Audit Manager supprime un compte membre dissocié des listes des comptes concernés par vos évaluations, vous n'êtes pas informé de cette modification. De plus, le compte membre dissocié n'est pas informé qu'Audit Manager n'est plus activé sur son compte.

Que se passe-t-il si je réassocie un compte membre à mon organisation ?

Lorsque vous réassociez un compte membre à votre organisation, ce compte n'est pas automatiquement ajouté à l'étendue de vos évaluations Audit Manager existantes. Toutefois, le compte de membre réassocié apparaît désormais comme éligible Compte AWS lorsque vous spécifiez les comptes concernés par vos évaluations.

- Pour les évaluations existantes, vous pouvez modifier manuellement l'étendue de l'évaluation pour ajouter le compte membre réassocié. Pour obtenir des instructions, veuillez consulter Étape 2 : Modifier Comptes AWS dans le champ d'application.
- Pour les nouvelles évaluations, vous pouvez ajouter le compte réassocié lors de la configuration de l'évaluation. Pour obtenir des instructions, veuillez consulter Étape 2 : Spécifier le champ Comptes AWS d'application.

Que se passe-t-il si je migre un compte membre d'une organisation vers une autre ?

Si Audit Manager est activé sur un compte membre dans l'organisation 1, mais que ce compte migre vers l'organisation 2, Audit Manager n'est pas activé pour l'organisation 2.

Résolution des problèmes liés à l'outil de recherche d'éléments probants

Utilisez les informations de cette page pour résoudre les problèmes courants liés à l'outil de recherche d'éléments probants dans Audit Manager.

Problèmes généraux liés à l'outil de recherche d'éléments probants

- Je ne parviens pas à activer l'outil de recherche d'éléments probants

- J'ai activé l'outil de recherche d'éléments probants, mais je ne vois pas les éléments probants passés dans mes résultats de recherche
- Je ne parviens pas à désactiver l'outil de recherche d'éléments probants
- Ma requête de recherche échoue

Problèmes liés aux rapports d'évaluation dans l'outil de recherche d'éléments probants

- Je ne parviens pas à générer plusieurs rapports d'évaluation à partir des résultats de ma recherche
- Je ne parviens pas à inclure des éléments probants spécifiques à partir des résultats de ma recherche
- Les résultats de ma recherche d'éléments probants ne sont pas tous inclus dans le rapport d'évaluation
- Je souhaite générer un rapport d'évaluation à partir des résultats de ma recherche, mais mon instruction de requête échoue
- Ressources supplémentaires

Problèmes d'exportation au format CSV dans l'outil de recherche d'éléments probants

- Mon exportation au format CSV a échoué
- Je ne parviens pas à exporter des éléments probants spécifiques à partir des résultats de ma recherche
- Je ne peux pas exporter plusieurs fichiers CSV à la fois

Je ne parviens pas à activer l'outil de recherche d'éléments probants

Les raisons courantes pour lesquelles vous ne pouvez pas activer l'outil de recherche d'éléments probants sont les suivantes :

Il vous manque des autorisations

Si vous essayez d'activer Evidence Finder pour la première fois, assurez-vous que vous disposez des autorisations requises pour activer Evidence Finder. Ces autorisations vous permettent de créer et de gérer un magasin de données sur les événements dans CloudTrail Lake, nécessaire pour répondre aux requêtes de recherche de preuves. Les autorisations vous permettent également d'exécuter des requêtes de recherche dans l'outil de recherche d'éléments probants.

Si vous avez besoin d'aide concernant les autorisations, contactez votre AWS administrateur. Si vous êtes AWS administrateur, vous pouvez copier la déclaration d'autorisation requise et la joindre à une politique IAM.

Vous utilisez votre compte de gestion Organizations

N'oubliez pas que vous pouvez utiliser votre compte de gestion pour activer l'outil de recherche d'éléments probants. Connectez-vous en tant que compte administrateur délégué, puis réessayez.

Vous avez précédemment désactivé l'outil de recherche d'éléments probants

La réactivation de l'outil de recherche d'éléments probants n'est actuellement pas prise en charge. Si vous avez précédemment désactivé l'outil de recherche d'éléments probants, vous ne pourrez pas l'activer à nouveau.

J'ai activé l'outil de recherche d'éléments probants, mais je ne vois pas les éléments probants passés dans mes résultats de recherche

Lorsque vous activez l'outil de recherche d'éléments probants, il faut jusqu'à 7 jours pour que toutes vos données d'éléments probants passés soient disponibles.

Au cours de cette période de 7 jours, un entrepôt de données d'événements est rempli avec vos données d'éléments probants des deux dernières années. Cela signifie que si vous utilisez l'outil de recherche d'éléments probants immédiatement après l'avoir activé, tous les résultats ne seront pas disponibles tant que le remplissage ne sera pas terminé.

Pour obtenir des instructions sur la façon de vérifier l'état du remblayage des données, consultezConfirmation du statut de chercheur de preuves .

Je ne parviens pas à désactiver l'outil de recherche d'éléments probants

Cela peut être dû à l'une des raisons suivantes.

Il vous manque des autorisations

Si vous essayez de désactiver l'outil de recherche de preuves, assurez-vous que vous disposez des autorisations requises pour désactiver l'outil de recherche de preuves. Ces autorisations vous permettent de mettre à jour et de supprimer un magasin de données d'événements dans CloudTrail Lake, ce qui est nécessaire pour désactiver l'outil de recherche de preuves.

Si vous avez besoin d'aide concernant les autorisations, contactez votre AWS administrateur. Si vous êtes AWS administrateur, vous pouvez copier la déclaration d'autorisation requise et la joindre à une politique IAM.

Une demande visant à activer l'outil de recherche d'éléments probants est toujours en cours

Lorsque vous demandez d'activer l'outil de recherche d'éléments probants, nous créons un entrepôt de données d'événements pour répondre aux requêtes de l'outil de recherche d'éléments probants. Vous ne pouvez pas désactiver l'outil de recherche d'éléments probants lors de la création de l'entrepôt de données d'événements.

Pour continuer, attendez que l'entrepôt de données d'événements soit créé, puis réessayez. Pour plus d'informations, consultez Confirmation du statut de chercheur de preuves .

Vous avez déjà demandé de désactiver l'outil de recherche d'éléments probants

Lorsque vous demandez de désactiver l'outil de recherche d'éléments probants, nous supprimons l'entrepôt de données d'événements utilisé pour les requêtes de l'outil de recherche d'éléments probants. Si vous essayez à nouveau de désactiver l'outil de recherche d'éléments probants alors que l'entrepôt de données d'événements est supprimé, un message d'erreur s'affiche.

Dans ce cas, aucune action n'est nécessaire. Attendez que l'entrepôt de données d'événements soit supprimé. Dès que cette opération est terminée, l'outil de recherche d'éléments probants est désactivé. Pour plus d'informations, consultez Confirmation du statut de chercheur de preuves .

Ma requête de recherche échoue

L'échec d'une requête de recherche peut être dû à l'une des raisons suivantes.

Il vous manque des autorisations

Vérifiez que l'utilisateur dispose des autorisations requises pour exécuter des requêtes de recherche et accéder aux résultats de recherche. Plus précisément, vous avez besoin d'autorisations pour les CloudTrail actions suivantes :

- StartQuery
- DescribeQuery
- CancelQuery
- GetQueryResults

Si vous avez besoin d'aide concernant les autorisations, contactez votre AWS administrateur. Si vous êtes AWS administrateur, vous pouvez copier la déclaration d'autorisation requise et la joindre à une politique IAM.

Vous exécutez le nombre maximal de requêtes

Vous pouvez exécuter jusqu'à 5 requêtes à la fois. Si vous exécutez le nombre maximal de requêtes simultanées, cela entraîne une erreur `MaxConcurrentQueriesException`. Si ce message d'erreur s'affiche, attendez une minute que certaines requêtes soient terminées, puis réexécutez la requête.

Votre instruction de requête contient une erreur de validation

Si vous utilisez l'API ou la CLI pour effectuer l'StartQueryopération CloudTrail Lake, assurez-vous que votre code `queryStatement` est valide. Si l'instruction de requête comporte des erreurs de validation, une syntaxe incorrecte ou des mots clés non pris en charge, cela se traduit par une `InvalidQueryStatementException`.

Pour plus d'informations sur l'écriture d'une requête, consultez Créer ou modifier une requête dans le Guide de l'utilisateur d'AWS CloudTrail .

Pour obtenir des exemples de syntaxe valide, consultez les exemples d'instructions de requêtes suivants qui peuvent être utilisés pour interroger un entrepôt de données d'événements dans Audit Manager.

Exemple 1 : Examiner les éléments probants et leur statut de conformité

Cet exemple permet de rechercher des éléments probants, quel que soit leur statut de conformité, dans toutes les évaluations prises en compte, dans une plage de dates spécifiée.

```
SELECT eventData.evidenceId, eventData.resourceArn,
 eventData.resourceComplianceCheck FROM $EDS_ID WHERE eventTime > '2022-11-02
 00:00:00.000' AND eventTime < '2022-11-03 00:00:00.000'
```

Exemple 2 : Déterminer les éléments probants non conformes d'un contrôle

Cet exemple permet de rechercher tous les éléments probantsnon conformes dans une plage de dates spécifiée pour une évaluation et un contrôle spécifiques.

```
SELECT * FROM $EDS_ID WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-
ff22gg44hh66' AND eventTime > '2022-10-27 22:05:00.000' AND eventTime
```

```
 < '2022-11-03 22:05:00.000' AND eventData.resourceComplianceCheck IN
 ('NON_COMPLIANT','FAILED','WARNING') AND eventData.controlId IN ('aa11bb22-cc33-
dd44-ee55-ff66gg77hh88')
```

Exemple 3 : Compter les éléments probants par nom

Cet exemple répertorie le nombre total d'éléments probants d'une évaluation dans une plage de dates spécifiée, groupés par nom et classés par nombre d'éléments probants.

```
SELECT eventData.eventName as eventName, COUNT(*) as totalEvidence FROM  $EDS_ID
 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime
 > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' GROUP BY
 eventData.eventName ORDER BY totalEvidence DESC
```

Exemple 4 : Explorer les éléments probants par source de données et par service

Cet exemple permet de rechercher tous les éléments probants dans une plage de dates spécifiée pour une source de données et un service spécifiques.

```
SELECT * FROM $EDS_ID WHERE eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.service IN ('dynamodb') AND
 eventData.dataSource IN ('AWS API calls')
```

Exemple 5 : Explorer les éléments probants conformes par source de données et domaine de contrôle

Cet exemple permet de rechercher des éléments probants conformes pour des domaines de contrôle spécifiques, lorsque les éléments probants proviennent d'une source de données autre qu'AWS Config.

```
 SELECT * FROM $EDS_ID WHERE eventData.resourceComplianceCheck IN
 ('PASSED','COMPLIANT') AND eventData.controlDomainName IN ('Logging and
 monitoring','Data security and privacy') AND eventData.dataSource NOT IN ('AWS
 Config')
```

Autres exceptions d'API

L'StartQueryAPI peut échouer pour plusieurs autres raisons. Pour obtenir la liste complète des erreurs possibles et leur description, consultez la section StartQuery Erreurs dans le guide de référence de l'AWS CloudTrail API.

Je ne parviens pas à générer plusieurs rapports d'évaluation à partir des résultats de ma recherche

Cette erreur est due à l'exécution d'un trop grand nombre de requêtes CloudTrail Lake en même temps.

Cette erreur peut se produire si vous regroupez les résultats de votre recherche et tentez de générer immédiatement des rapports d'évaluation pour chaque élément de ligne de vos résultats regroupés. Lorsque vous obtenez les résultats de votre recherche et que vous générez un rapport d'évaluation, chaque action invoque une requête. Vous ne pouvez exécuter que 5 requêtes à la fois. Si vous exécutez le nombre maximal de requêtes simultanées, l'erreur `MaxConcurrentQueriesException` est renvoyée.

Pour éviter cette erreur, assurez-vous de ne pas générer trop de rapports d'évaluation à la fois. Si vous exécutez le nombre maximal de requêtes simultanées, l'erreur `MaxConcurrentQueriesException` est renvoyée. Si ce message d'erreur s'affiche, attendez quelques minutes que vos rapports d'évaluation en cours soient terminés.

Vous pouvez vérifier le statut de vos rapports d'évaluation depuis la page du centre de téléchargement de la console Audit Manager. Une fois vos rapports terminés, revenez à vos résultats regroupés dans l'outil de recherche d'éléments probants. Vous pouvez ensuite continuer à obtenir les résultats et à générer un rapport d'évaluation pour chaque élément de ligne.

Je ne parviens pas à inclure des éléments probants spécifiques à partir des résultats de ma recherche

Tous les résultats de votre recherche sont inclus dans le rapport d'évaluation. Vous ne pouvez pas ajouter de lignes individuelles de manière sélective à partir de votre ensemble de résultats de recherche.

Si vous souhaitez uniquement inclure des résultats de recherche spécifiques dans le rapport d'évaluation, nous vous recommandons de modifier vos filtres de recherche actuels. Ainsi, vous pouvez affiner vos résultats pour cibler uniquement les éléments probants que vous souhaitez inclure dans le rapport.

Les résultats de ma recherche d'éléments probants ne sont pas tous inclus dans le rapport d'évaluation

Lorsque vous générez un rapport d'évaluation, le nombre d'éléments probants que vous pouvez ajouter est limité. La limite dépend de votre évaluation, Région AWS de la région du compartiment S3 utilisée comme destination de votre rapport d'évaluation et du fait que votre évaluation utilise ou non un service géré par le client AWS KMS key.

1. La limite est de 22 000 pour les rapports d'une même région (dans le cas où le compartiment S3 et l'évaluation se trouvent dans la même Région AWS)
2. La limite est de 3 500 pour les rapports interrégionaux (dans le cas où le compartiment S3 et l'évaluation se trouvent dans des Régions AWS différentes)
3. La limite est de 3 500 si l'évaluation utilise une clé KMS gérée par le client

Si vous dépassez cette limite, le rapport est quand même créé. Toutefois, Audit Manager ajoute uniquement les 3 500 ou 22 000 premiers éléments probants au rapport.

Pour éviter ce problème, nous vous recommandons de modifier vos filtres de recherche actuels. De cette façon, vous pouvez réduire les résultats de votre recherche en ciblant un plus petit nombre d'éléments probants. Si nécessaire, vous pouvez répéter cette méthode et générer plusieurs rapports d'évaluation au lieu d'un seul rapport plus volumineux.

Je souhaite générer un rapport d'évaluation à partir des résultats de ma recherche, mais mon instruction de requête échoue

Si vous utilisez l'CreateAssessmentReportAPI et que votre instruction de requête renvoie une exception de validation, consultez le tableau ci-dessous pour savoir comment y remédier.

> **Note**
>
> Même si une instruction de requête fonctionne CloudTrail, il est possible que la même requête ne soit pas valide pour la génération du rapport d'évaluation dans Audit Manager. Cela est dû à certaines différences dans la validation des requêtes entre les deux services.

Clause	Problème	Solution	Remarques
`SELECT`	La clause `SELECT` contient un nom de colonne	Supprimez la clause `SELECT` et remplacez-la par `SELECT eventJson` .	Seule la clause `SELECT eventJson` est prise en charge. Cette validation est gérée par Audit Manager.
`FROM`	La clause `FROM` contient un identifiant d'entrepôt de données d'événements non valide or L'identifiant d'entrepôt de données d'événements fourni ne correspond pas à l'identifiant d'entrepôt de données d'événements dans vos paramètres Audit Manager	Supprimez la clause `FROM` et remplacez-la par `FROM` *`edsID`*, où la valeur de `edsID` correspond à l'ID d'entrepôt de données d'événements spécifié dans vos paramètres Audit Manager. Vous pouvez récupérer l'ARN de l'entrepôt de données d'événements à partir de vos paramètres Audit Manager. Pour plus d'informations, consultez GetSettingsla référence de AWS Audit Manager l'API.	Cette validation est gérée par Audit Manager.
`GROUP BY`	La clause `GROUP BY` est présente dans la requête	Supprimez la clause `GROUP BY`.	Cette validation est gérée par Audit Manager.
`HAVING`	La clause `HAVING` est présente dans la requête	Supprimez la clause `HAVING`.	Cette validation est gérée par Audit Manager.
`LIMIT`	La clause `LIMIT` contient une valeur	Si la clause `LIMIT` existe, assurez-vous que sa valeur est	Dans la console, il n'y a aucune limite au nombre

Clause	Problème	Solution	Remarques
	qui dépasse la limite maximale autorisée	égale ou inférieure à la limite maximale prise en charge : • Pour les rapports d'une même région, la limite est de 22 000 • Pour les rapports interrégionaux, la limite est de 3 500 • Pour les rapports où l'évaluation associée utilise un système géré par le client AWS KMS key, la limite est de 3 500	de résultats d'éléments probants pouvant être renvoyés. Toutefois, lors de la génération d'un rapport d'évaluation, une limite s'applique au nombre d'éléments probants que vous pouvez inclure. Si aucune valeur `LIMIT` n'est fournie dans votre instruction de requête, les limites maximales par défaut sont appliquées. Cette validation est gérée par Audit Manager.
`ORDER BY`	La clause `ORDER BY` contient des fonctions d'agrégation ou des alias qui ne sont pas présents dans la clause `SELECT`	Assurez-vous que la clause `ORDER BY` ne contient aucune condition utilisant des fonctions d'agrégation ou des alias.	Cette validation est gérée par l' CloudTrail StartQuery API.

Clause	Problème	Solution	Remarques
`WHERE`	La clause `WHERE` contient plusieurs `assessmentId` or La clause `WHERE` contient un `assessmentId` qui ne correspond pas à l'`assessmentId` de votre demande `createAssessmentReport` or La clause `WHERE` contient un nom de colonne non pris en charge	Assurez-vous qu'un seul assessmentID est spécifié et qu'il correspond au paramètre assessmentID que vous avez spécifié dans la demande d'API `createAssessmentReport` . Supprimez tous les noms de colonnes non pris en charge.	Cette validation est gérée par l' CloudTrail StartQuery API.

Exemples

Les exemples suivants montrent comment utiliser le `queryStatement` paramètre lors de l'appel de l'CreateAssessmentReportopération. Avant d'utiliser ces requêtes, remplacez le *`texte de l'espace réservé`* par vos propres valeurs `edsId` et `assessmentId`.

Exemple 1 : Créer un rapport (la limite de même région s'applique)

Cet exemple crée un rapport qui inclut les résultats des compartiments S3 créés entre le 22 et le 23 janvier 2022.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-01-22 00:00:00.000' AND
 eventTime < '2022-01-23 00:00:00.000' AND eventName='CreateBucket' LIMIT 22000
```

Exemple 2 : Créer un rapport (la limite interrégionale s'applique)

Cet exemple crée un rapport qui inclut tous les résultats de l'entrepôt de données d'événements et de l'évaluation spécifiés, sans qu'aucune plage de dates soit spécifiée.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 7000
```

Exemple 3 : Créer un rapport (sous la limite par défaut)

Cet exemple crée un rapport qui inclut tous les résultats de l'entrepôt de données d'événements et de l'évaluation spécifiés, avec une limite inférieure au maximum par défaut.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 2000
```

Ressources supplémentaires

La page suivante contient des conseils généraux pour la résolution des problèmes liés aux rapports d'évaluation :

- Résolution des problèmes liés aux rapports d'évaluation

Mon exportation au format CSV a échoué

Votre exportation au format CSV peut échouer pour plusieurs raisons. Vous pouvez résoudre ce problème en vérifiant les causes les plus fréquentes.

Tout d'abord, vérifiez que vous remplissez les conditions requises pour utiliser la fonctionnalité d'exportation au format CSV :

Vous avez activé l'outil de recherche d'éléments probants avec succès

Si vous n'avez pas activé l'outil de recherche d'éléments probants, vous ne pouvez pas exécuter de requête de recherche et exporter les résultats de votre recherche.

Le remplissage de votre entrepôt de données d'événements est terminé

Si vous utilisez l'outil de recherche d'éléments probants immédiatement après l'avoir activé et que le remplissage des éléments probants est toujours en cours, il se peut que certains résultats ne

soient pas disponibles. Pour vérifier l'état du remblayage, voirConfirmation du statut de chercheur de preuves .

Votre requête de recherche a réussi

Audit Manager ne peut pas exporter les résultats d'une requête ayant échoué. Pour résoudre les problèmes liés à l'échec d'une requête, consultez Ma requête de recherche échoue.

Après avoir vérifié que vous remplissez les conditions requises, utilisez la liste de contrôle suivante pour vérifier les problèmes potentiels :

1. Vérifiez le statut de votre requête de recherche :
   a. La requête a-t-elle été annulée ? L'outil de recherche d'éléments probants affiche des résultats partiels traités avant l'annulation de la requête. Toutefois, Audit Manager n'exporte pas les résultats partiels vers votre compartiment S3 ou le centre de téléchargement.
   b. La requête est-elle en cours d'exécution depuis plus d'une heure ? Les requêtes qui s'exécutent pendant plus d'une heure peuvent prendre fin. L'outil de recherche d'éléments probants affiche des résultats partiels traités avant l'expiration de la requête. Toutefois, Audit Manager n'exporte pas de résultats partiels. Pour éviter un délai d'attente, vous pouvez réduire la quantité de preuves numérisées en spécifiant une plage Modification des filtres de recherche de temps plus étroite.
2. Vérifiez le nom et l'URI du compartiment S3 de destination de votre exportation :
   a. Le compartiment que vous avez spécifié existe-t-il ? Si vous avez saisi manuellement l'URI d'un compartiment, assurez-vous de ne pas avoir commis d'erreur de frappe. Une faute de frappe ou un URI incorrect peut générer une erreur `RESOURCE_NOT_FOUND` lorsqu'Audit Manager tente d'exporter le fichier CSV vers Amazon S3.
3. Vérifiez les autorisations du compartiment S3 de destination de votre exportation :
   a. Disposez-vous d'autorisations d'écriture pour le compartiment S3 ? Vous devez disposer d'un accès en écriture pour le compartiment S3 que vous utilisez comme destination d'exportation. Plus précisément, la politique d'autorisation IAM doit inclure une `s3:PutObject` action et l'ARN du bucket, et la liste CloudTrail en tant que principal de service. Nous fournissons un exemple de politique que vous pouvez utiliser.
4. Vérifiez si certaines de vos Région AWS informations ne correspondent pas :
   a. La Région AWS clé gérée par votre client correspond-elle à celle Région AWS de votre évaluation ? Si vous avez fourni une clé gérée par le client pour le chiffrement des données, celle-ci doit se trouver dans la même Région AWS que celle de votre évaluation. Pour obtenir

des instructions sur la modification de la clé KMS, consultezConfiguration de vos paramètres de chiffrement des données.

5. Vérifiez les autorisations de votre compte administrateur délégué :
   a. La clé gérée par le client dans vos paramètres Audit Manager accorde-t-elle des autorisations à votre administrateur délégué ? Si vous utilisez un compte administrateur délégué et que vous avez spécifié une clé gérée par le client pour le chiffrement des données, assurez-vous que l'administrateur délégué a accès à cette clé KMS. Pour obtenir des instructions, consultez Autoriser des utilisateurs d'autres comptes à utiliser une clé KMS dans le Guide du développeur d'AWS Key Management Service . Pour vérifier et modifier vos paramètres de chiffrement dans Audit Manager, consultezConfiguration de vos paramètres de chiffrement des données.

> **Note**
>
> Si vous modifiez vos paramètres de chiffrement des données Audit Manager, ces modifications s'appliqueront aux nouvelles évaluations que vous créerez à l'avenir. Cela inclut tous les fichiers CSV que vous exportez à partir de vos nouvelles évaluations.
> Les modifications ne s'appliquent pas aux évaluations existantes que vous avez créées avant de modifier vos paramètres de chiffrement. Cela inclut les nouvelles exportations au format CSV à partir d'évaluations existantes, en plus des exportations au format CSV existantes. Les évaluations existantes, ainsi que toutes leurs exportations au format CSV, continuent d'utiliser l'ancienne clé KMS. Si l'identité IAM qui exporte le fichier CSV n'est pas autorisée à utiliser l'ancienne clé KMS, vous pouvez accorder des autorisations au niveau de la stratégie de clé.

Je ne parviens pas à exporter des éléments probants spécifiques à partir des résultats de ma recherche

Tous les résultats de votre recherche sont inclus dans les résultats.

Si vous souhaitez inclure uniquement des éléments probants spécifiques dans le fichier CSV, nous vous recommandons de modifier vos filtres de recherche actuels. Ainsi, vous pouvez affiner vos résultats pour cibler uniquement les éléments probants que vous souhaitez exporter.

Je ne peux pas exporter plusieurs fichiers CSV à la fois

Cette erreur est due à l'exécution d'un trop grand nombre de requêtes CloudTrail Lake en même temps.

Cela peut se produire si vous regroupez les résultats de votre recherche et tentez d'exporter immédiatement un fichier CSV pour chaque élément de ligne de vos résultats regroupés. Lorsque vous obtenez les résultats de votre recherche et que vous exportez un fichier CSV, chacune de ces actions invoque une requête. Vous ne pouvez exécuter que cinq requêtes à la fois. Si vous exécutez le nombre maximal de requêtes simultanées, l'erreur `MaxConcurrentQueriesException` est renvoyée.

Pour éviter cette erreur, assurez-vous de ne pas exporter trop de fichiers CSV à la fois.

Pour résoudre cette erreur, attendez que vos exportations au format CSV en cours soient terminées. La plupart des exportations prennent quelques minutes. Toutefois, si vous exportez une très grande quantité de données, l'exportation peut prendre jusqu'à une heure. N'hésitez pas à quitter l'outil de recherche d'éléments probants pendant que l'exportation est en cours.

Vous pouvez vérifier le statut de l'exportation depuis le centre de téléchargement de la console Audit Manager. Une fois que vos fichiers exportés sont prêts, revenez à vos résultats regroupés dans l'outil de recherche d'éléments probants. Vous pouvez ensuite continuer à obtenir les résultats et à exporter un fichier CSV pour chaque élément de ligne.

Résolution des problèmes liés au framework

Vous pouvez utiliser les informations de cette page pour résoudre les problèmes courants liés au framework dans Audit Manager.

Problèmes généraux liés au cadre

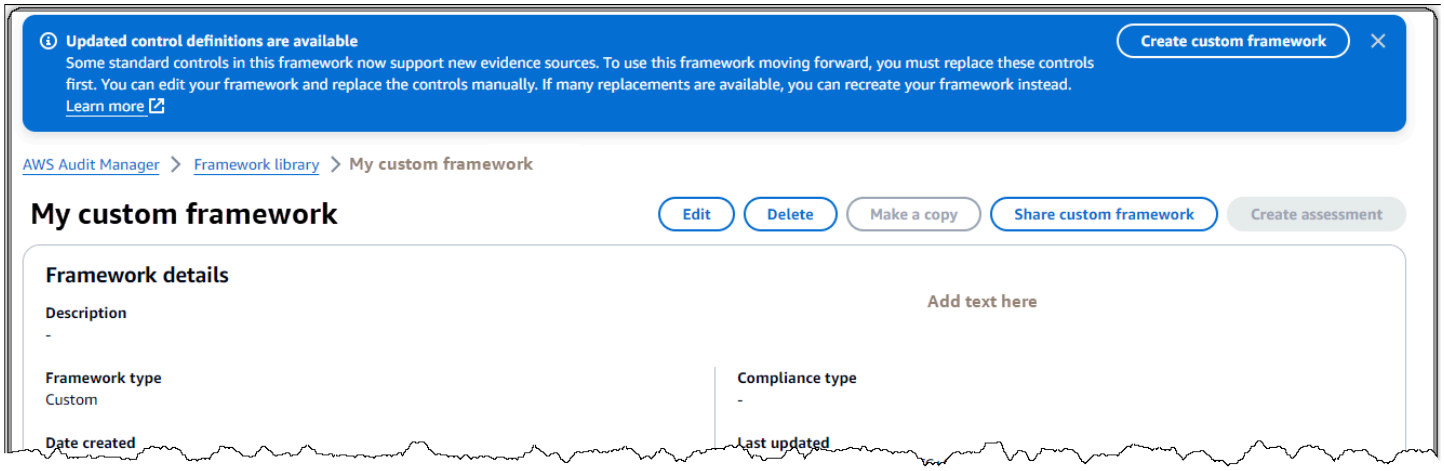
- Sur la page de détails de mon framework personnalisé, je suis invité à recréer mon framework personnalisé
- Je ne parviens pas à faire une copie de mon framework personnalisé ni à l'utiliser pour créer une évaluation

Problèmes de partage du cadre

- Le statut de ma demande de partage envoyée s'affiche comme Échec
- Ma demande de partage est accompagnée d'un point bleu. Qu'est-ce que cela signifie ?
- Mon framework partagé comporte des contrôles qui utilisent des AWS Config règles personnalisées comme source de données. Le destinataire peut-il collecter des éléments probants pour ces contrôles ?

- J'ai mis à jour une règle personnalisée utilisée dans un cadre partagé. Dois-je prendre des mesures ?

Sur la page de détails de mon framework personnalisé, je suis invité à recréer mon framework personnalisé



Si vous voyez un message indiquant que des définitions de contrôle mises à jour sont disponibles, cela indique qu'Audit Manager fournit désormais de nouvelles définitions pour certains des contrôles standard de votre framework personnalisé.

Les contrôles standard peuvent désormais collecter des preuves auprès deAWS managed source. Cela signifie que chaque fois qu'Audit Manager met à jour les sources de données sous-jacentes pour un contrôle commun ou principal, la même mise à jour est automatiquement appliquée aux contrôles standard associés. Cela vous permet de garantir une conformité continue à mesure que l'environnement de conformité du cloud évolue. Pour vous assurer de tirer parti de ces sources AWS gérées, nous vous recommandons de remplacer les contrôles dans votre infrastructure personnalisée.

Dans votre framework personnalisé, Audit Manager indique les contrôles pour lesquels des remplacements sont disponibles. Vous devrez remplacer ces contrôles avant de pouvoir créer une copie de votre framework personnalisé ou créer une évaluation à partir de celui-ci. La prochaine fois que vous modifierez votre cadre personnalisé, nous vous demanderons de remplacer ces contrôles par toute autre modification que vous souhaiteriez apporter.

Il existe deux manières de remplacer les contrôles dans votre cadre personnalisé :

1. Recréez votre framework personnalisé

Si un grand nombre de contrôles peuvent être remplacés, nous vous recommandons de recréer votre structure personnalisée. Il s'agit probablement de la meilleure option si votre framework personnalisé est basé sur un framework standard.

- Supposons, par exemple, que vous ayez créé votre framework personnalisé en utilisant NIST SP 800-53 Rév. 5 comme point de départ. Ce cadre standard comporte 1007 contrôles standard, et vous avez ajouté 20 contrôles personnalisés.
- Dans ce cas, l'option la plus efficace consiste à rechercher `NIST 800-53 (Rev. 5) Low-Moderate-High` dans la bibliothèque du framework et à en faire une copie modifiable. Au cours de ce processus, vous pouvez ajouter les 20 contrôles personnalisés que vous utilisiez auparavant. Comme vous utilisez désormais la dernière définition du framework standard comme point de départ, votre framework personnalisé hérite automatiquement des dernières définitions pour l'ensemble des 1007 contrôles standard.

2. Modifiez votre framework personnalisé

Si des remplacements sont disponibles pour un petit nombre de contrôles, nous vous recommandons de modifier votre structure personnalisée et de remplacer les contrôles manuellement.

- Supposons, par exemple, que vous ayez créé votre framework personnalisé à partir de zéro. Dans votre cadre personnalisé, vous avez ajouté 20 contrôles personnalisés que vous avez créés vous-même et huit contrôles standard issus du cadre ACSC Essential Eight standard.
- Dans ce cas, étant donné que des mises à jour sont disponibles pour un maximum de huit contrôles, l'option la plus efficace consiste à modifier votre structure personnalisée et à remplacer ces contrôles un par un. Pour plus d'informations, consultez la procédure suivante.

Pour remplacer manuellement les contrôles dans votre cadre personnalisé

Pour remplacer manuellement les contrôles dans votre cadre personnalisé

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Framework library, puis choisissez l'onglet Custom frameworks.
3. Sélectionnez le framework que vous souhaitez modifier, choisissez Actions, puis Modifier.
4. Sur la page Modifier les détails du framework, choisissez Next.

5. Sur la page Modifier les ensembles de contrôles, passez en revue le nom de chaque ensemble de contrôles pour voir si des remplacements sont disponibles pour certains de ses contrôles.
6. Choisissez un ensemble de commandes concerné pour l'étendre et identifiez les commandes à remplacer.

   > **Tip**
   >
   > Pour identifier plus rapidement les contrôles, entrez **`Replacement available`** dans le champ de recherche.

7. Supprimez les contrôles concernés en cochant la case et en choisissant Supprimer du jeu de contrôles.
8. Ajoutez à nouveau les mêmes commandes. Cette action remplace les contrôles que vous venez de supprimer par la dernière définition de contrôle.

   a. Sous Ajouter des contrôles, utilisez la liste déroulante des types de contrôle et sélectionnez Contrôles standard.

   b. Trouvez le remplacement de la commande que vous venez de retirer.

      > **Tip**
      >
      > Dans certains cas, le nom du contrôle de remplacement peut ne pas être exactement le même que celui d'origine. Dans ce cas, le nom du contrôle de remplacement est susceptible d'être très similaire à l'original. Dans de rares cas, une commande peut être remplacée par deux commandes (ou inversement).
      > Si vous ne trouvez pas de commande de remplacement, nous vous recommandons d'effectuer une recherche partielle. Pour ce faire, entrez une partie du nom du contrôle d'origine ou un mot clé qui représente ce que vous recherchez. Vous pouvez également effectuer une recherche par type de conformité pour affiner davantage la liste des résultats.

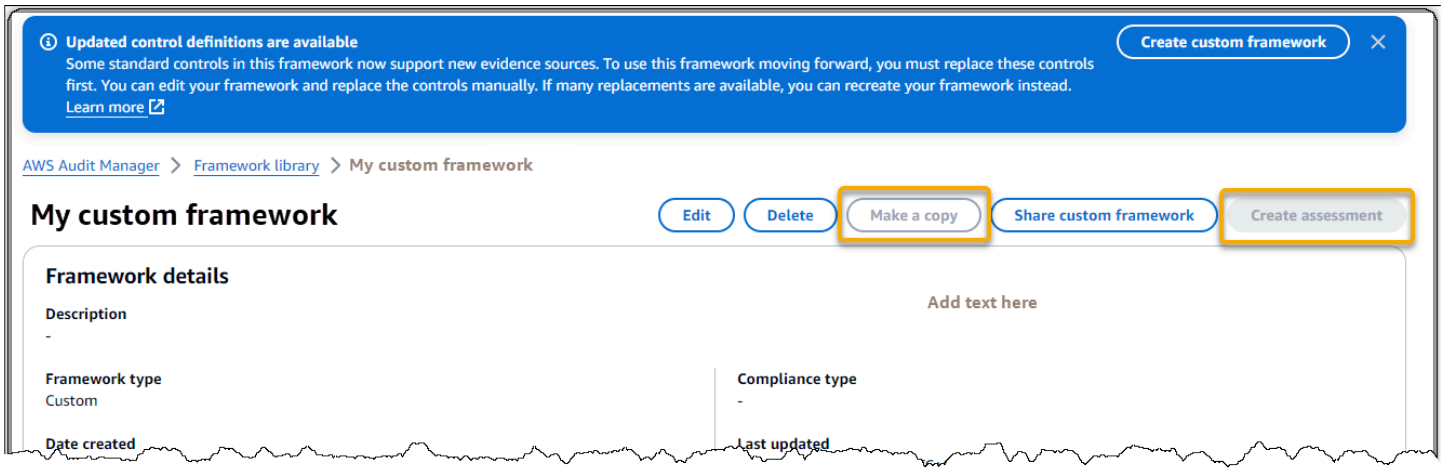
   c. Cochez la case située à côté d'un contrôle et choisissez Ajouter au jeu de contrôles.

   d. Dans la fenêtre contextuelle qui apparaît, choisissez Ajouter pour confirmer.

9. Répétez les étapes 6 à 8 selon les besoins jusqu'à ce que vous ayez remplacé toutes les commandes.
10. Choisissez Suivant.

11. Sur la page Réviser et enregistrer, choisissez Enregistrer les modifications.

Je ne parviens pas à faire une copie de mon framework personnalisé ni à l'utiliser pour créer une évaluation



Si les boutons Créer une copie et Créer une évaluation ne sont pas disponibles sur la page de détails du framework, cela signifie que vous devez remplacer certains contrôles de votre framework personnalisé.

Pour obtenir des instructions sur la procédure à suivre, consultezSur la page de détails de mon framework personnalisé, je suis invité à recréer mon framework personnalisé.

Le statut de ma demande de partage envoyée s'affiche comme Échec

Si vous essayez de partager un cadre personnalisé et que l'opération échoue, nous vous recommandons de vérifier les points suivants :

1. Assurez-vous qu'Audit Manager est activé dans la région du destinataire Compte AWS et dans la région spécifiée. Pour obtenir la liste des AWS Audit Manager régions prises en charge, consultez les AWS Audit Manager points de terminaison et les quotas dans le manuel Amazon Web Services General Reference.
2. Assurez-vous d'avoir saisi le bon Compte AWS identifiant lorsque vous avez indiqué le compte du destinataire.
3. Assurez-vous que vous n'avez pas indiqué de compte AWS Organizations de gestion comme destinataire. Vous pouvez partager un cadre personnalisé avec un administrateur délégué, mais si vous essayez de partager un cadre personnalisé avec un compte de gestion, l'opération échoue.

4. Si vous utilisez une clé gérée par le client pour chiffrer vos données Audit Manager, assurez-vous que votre clé KMS est activée. Si votre clé KMS est désactivée et que vous essayez de partager un cadre personnalisé, l'opération échoue. Pour obtenir des instructions sur l'activation d'une clé KMS désactivée, consultez Activation et désactivation des clés dans le Guide du développeur d'AWS Key Management Service .

Ma demande de partage est accompagnée d'un point bleu. Qu'est-ce que cela signifie ?

Une notification à point bleu indique qu'une demande de partage nécessite votre attention.

Notifications à point bleu destinées aux expéditeurs

Un point de notification bleu apparaît à côté des demandes de partage envoyées dont le statut est Expiration. Audit Manager affiche la notification à point bleu afin que vous puissiez rappeler au destinataire de donner suite à la demande de partage avant son expiration.

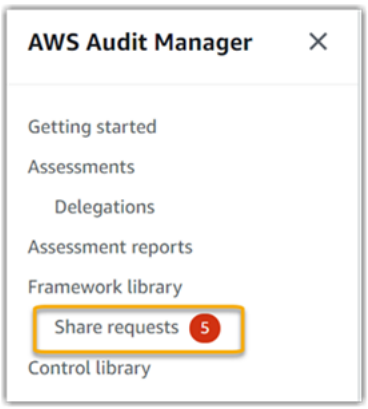
Pour que le point bleu de notification disparaisse, le destinataire doit accepter ou refuser la demande. Le point bleu disparaît également si vous révoquez la demande de partage.

Vous pouvez utiliser la procédure suivante pour vérifier si des demandes de partage arrivent à expiration et envoyer un rappel facultatif au destinataire pour qu'il prenne les mesures nécessaires.

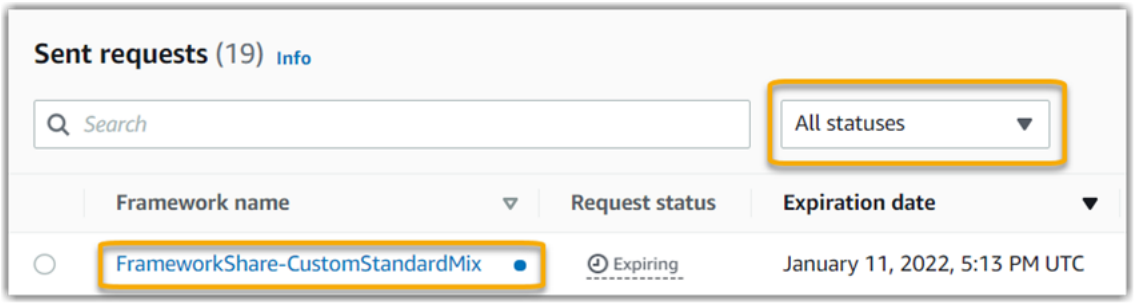
Pour afficher les notifications relatives aux demandes envoyées

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Si vous avez reçu une notification de demande de partage, Audit Manager affiche un point rouge à côté de l'icône du menu de navigation.

3. Développez le volet de navigation et regardez à côté de Demandes de partage. Un badge de notification indique le nombre de demandes de partage nécessitant une attention particulière.



4. Choisissez Demandes de partage, puis sélectionnez l'onglet Demandes envoyées.
5. Recherchez le point bleu pour identifier les demandes de partage qui expireront dans les 30 prochains jours. Vous pouvez également consulter les demandes de partage arrivant à expiration en sélectionnant Expiration dans le menu déroulant du filtre Tous les statuts.



6. (Facultatif) Rappelez au destinataire qu'il doit donner suite à la demande de partage avant son expiration. Cette étape est facultative, car Audit Manager envoie une notification dans la console pour informer le destinataire lorsqu'une demande de partage est active ou expire. Cependant, vous pouvez également envoyer votre propre rappel au destinataire en utilisant votre canal de communication préféré.

Notifications à point bleu destinées aux destinataires

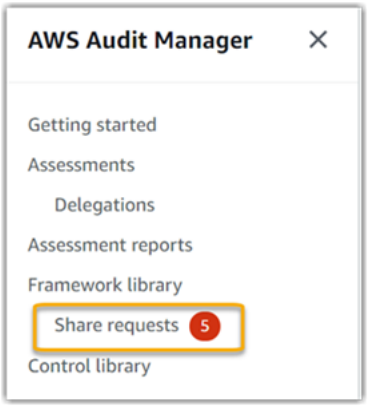
Un point bleu de notification apparaît à côté des demandes de partage reçues dont le statut est Actif ou Expiration. Audit Manager affiche la notification à point bleu pour vous rappeler de donner suite à la demande de partage avant son expiration. Pour que le point de notification bleu disparaisse, vous devez accepter ou refuser la demande. Le point bleu disparaît également si l'expéditeur révoque la demande de partage.

Vous pouvez utiliser la procédure suivante pour vérifier les demandes de partage actives et en cours d'expiration.

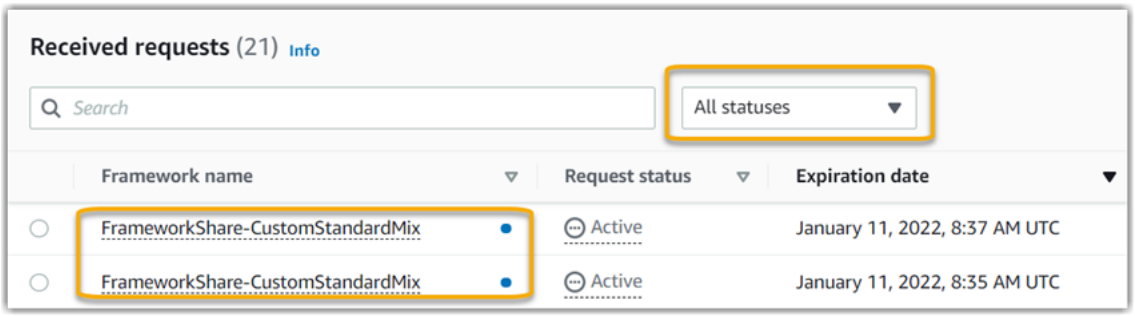
Pour afficher les notifications relatives aux demandes reçues

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Si vous avez reçu une notification de demande de partage, Audit Manager affiche un point rouge à côté de l'icône du menu de navigation.

3. Développez le volet de navigation et regardez à côté de Demandes de partage. Un badge de notification indique le nombre de demandes de partage qui nécessitent votre attention.



4. Choisissez Demandes de partage. Par défaut, cette page s'ouvre dans l'onglet Demandes reçues.
5. Identifiez les demandes de partage qui nécessitent une action de votre part en recherchant les éléments marqués d'un point bleu.



6. (Facultatif) Pour afficher uniquement les demandes qui expireront dans les 30 prochains jours, recherchez la liste déroulante Tous les statuts et sélectionnez Arrive à expiration.

Mon framework partagé comporte des contrôles qui utilisent des AWS Config règles personnalisées comme source de données. Le destinataire peut-il collecter des éléments probants pour ces contrôles ?

Oui, votre destinataire peut collecter des éléments probants pour ces contrôles, mais quelques étapes sont nécessaires pour y parvenir.

Pour qu'Audit Manager collecte des preuves en utilisant une AWS Config règle comme mappage de source de données, les conditions suivantes doivent être vraies. Ces critères s'appliquent à la fois aux règles gérées et aux règles personnalisées.

- La règle doit exister dans l' AWS environnement du destinataire.
- La règle doit être activée dans l' AWS environnement du destinataire.

N'oubliez pas que les AWS Config règles de votre compte n'existent probablement pas déjà dans l' AWS environnement du destinataire. De plus, lorsque le destinataire accepte la demande de partage, Audit Manager ne recrée aucune de vos règles personnalisées dans son compte. Pour que le destinataire puisse collecter des preuves en utilisant vos règles personnalisées comme mappage de sources de données, il doit créer les mêmes règles personnalisées dans son instance de AWS Config. Une fois que le destinataire a créé puis activé les règles AWS Config, Audit Manager peut collecter des preuves à partir de cette source de données.

Nous vous recommandons de communiquer avec le destinataire pour lui faire savoir si des AWS Config règles personnalisées doivent être créées dans son instance de AWS Config.

J'ai mis à jour une règle personnalisée utilisée dans un cadre partagé. Dois-je prendre des mesures ?

Pour les mises à jour des règles au sein de votre AWS environnement

Lorsque vous mettez à jour une règle personnalisée dans votre AWS environnement, aucune action n'est nécessaire dans Audit Manager. Audit Manager détecte et gère les mises à jour des règles de la manière décrite dans le tableau suivant. Audit Manager ne vous avertit pas lorsqu'une mise à jour des règles est détectée.

Scénario	Ce que fait Audit Manager	Ce que vous devez faire
Une règle personnalisée est mise à jour dans votre instance de AWS Config.	Audit Manager continue de rapporter les résultats relatifs à cette règle à l'aide de la définition de règle mise à jour.	Aucune action n'est nécessaire.
Une règle personnalisée est supprimée dans votre instance de AWS Config.	Audit Manager arrête de rapporter les résultats relatifs à la règle supprimée.	Aucune action n'est nécessaire. Si vous le souhaitez, vous pouvez modifier les contrôles personnalisés qui ont utilisé la règle supprimée comme mappage de source de données. Vous pouvez ensuite retirer la règle supprimée pour nettoyer les paramètres de source de données de votre contrôle. Dans le cas contraire, le nom de la règle supprimée reste un mappage de source de données inutilisé.

Pour les mises à jour des règles en dehors de votre AWS environnement

Dans l' AWS environnement du destinataire, Audit Manager ne détecte pas la mise à jour des règles. Cela est dû au fait que les expéditeurs et les destinataires travaillent chacun dans AWS des environnements distincts. Le tableau suivant fournit les actions recommandées pour ce scénario.

Votre rôle	Scénario	Action recommandée
Expédi r	• Vous avez partagé un cadre qui utilise des règles personnalisées comme mappage de source de données.	Contactez le destinataire pour l'informer de la mise à jour. Il peut ainsi effectuer la même mise à jour et rester synchronisé avec la dernière définition de règle.

Votre rôle	Scénario	Action recommandée
	• Après avoir partagé le framework, vous avez mis à jour ou supprimé l'une de ces règles dans AWS Config.	
Destinataire	• Vous avez accepté un cadre partagé qui utilise des règles personnalisées comme mappage de source de données. • Après avoir recréé les règles personnalisées dans votre instance de AWS Config, l'expéditeur a mis à jour ou supprimé l'une de ces règles.	Effectuez la mise à jour de la règle correspondante dans votre propre instance de AWS Config.

Résolution des problèmes liés aux notifications

Vous pouvez utiliser les informations de cette page pour résoudre les problèmes courants de notification dans Audit Manager.

Rubriques

J'ai spécifié une rubrique Amazon SNS dans Audit Manager, mais je ne reçois aucune notification

Si votre rubrique Amazon SNS traite du chiffrement côté serveur (SSE), il se peut que vous ne disposiez pas des autorisations requises pour votre politique en matière de clés. AWS KMS AWS KMS Il se peut également que vous ne receviez pas de notifications si vous n'avez pas abonné un point de terminaison à votre rubrique.

Si vous ne recevez pas de notifications, vérifiez que vous avez effectué les opérations suivantes :

- Vous avez joint la politique d'autorisation requise à votre clé KMS. Pour un exemple de politique que vous pouvez utiliser, consultezExemple 2 (autorisations pour la clé KMS associée à la rubrique SNS).
- Vous avez abonné un point de terminaison à la rubrique via laquelle les notifications sont envoyées. Lorsque vous abonnez un point de terminaison de messagerie à une rubrique, vous recevez un e-mail vous demandant de confirmer votre abonnement. Vous devez confirmer votre abonnement pour commencer à recevoir des notifications par e-mail. Pour plus d'informations, consultez Mise en route dans le Guide du développeur d'Amazon SNS.

J'ai spécifié une rubrique FIFO, mais je ne reçois pas de notifications dans l'ordre prévu

Audit Manager prend en charge l'envoi de notifications aux rubriques FIFO SNS. Cependant, l'ordre dans lequel Audit Manager envoie les notifications à vos rubriques FIFO n'est pas garanti.

Résolution des problèmes liés aux autorisations et à l'accès

Vous pouvez utiliser les informations de cette page pour résoudre les problèmes courants d'autorisation dans Audit Manager.

Rubriques

- J'ai suivi la procédure de configuration d'Audit Manager, mais je n'ai pas suffisamment de privilèges IAM
- J'ai désigné une personne comme responsable de l'audit, mais elle n'a toujours pas un accès complet à l'évaluation. Pourquoi est-ce le cas ?
- Je ne parviens pas à exécuter une action dans Audit Manager
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder aux ressources de mon Audit Manager
- Je vois un message d'erreur « Accès refusé » alors que je dispose des autorisations d'Audit Manager requises
- Ressources supplémentaires

J'ai suivi la procédure de configuration d'Audit Manager, mais je n'ai pas suffisamment de privilèges IAM

L'utilisateur, le rôle ou le groupe que vous utilisez pour accéder à Audit Manager doit disposer des autorisations requises. De plus, votre politique basée sur l'identité ne doit pas être trop restrictive. Dans le cas contraire, la console ne fonctionnera pas comme prévu. Ce guide fournit un exemple de politique que vous pouvez utiliserAjoutez les autorisations minimales requises pour activer Audit Manager. Selon votre cas d'utilisation, vous aurez peut-être besoin d'autorisations plus larges et moins restrictives. Par exemple, nous recommandons aux responsables de l'audit de disposer d'un accès administrateur. Cela leur permet de modifier les paramètres d'Audit Manager et de gérer des ressources telles que les évaluations, les cadres, les contrôles et les rapports d'évaluation. D'autres utilisateurs, comme les délégués, peuvent n'avoir besoin que d'un accès de gestion ou d'un accès en lecture seule.

Assurez-vous d'ajouter les autorisations appropriées pour votre utilisateur, votre rôle ou votre groupe. Pour les responsables de l'audit, la politique recommandée est AWSAuditManagerAdministratorAccess. Pour les délégués, vous pouvez utiliser l'exemple de politique d'accès à la gestion fourni sur la page d'exemples de politiques IAM. Vous pouvez utiliser ces exemples de politiques comme point de départ et apporter les modifications nécessaires pour répondre à vos besoins.

Nous vous recommandons de prendre le temps de personnaliser vos autorisations en fonction de vos besoins spécifiques. Si vous avez besoin d'aide concernant les autorisations IAM, contactez votre administrateur ou AWS Support.

J'ai désigné une personne comme responsable de l'audit, mais elle n'a toujours pas un accès complet à l'évaluation. Pourquoi est-ce le cas ?

Le fait de désigner une personne comme responsable de l'audit ne suffit pas pour lui donner un accès complet à une évaluation. Les responsables de l'audit doivent également disposer des autorisations IAM nécessaires pour accéder aux ressources d'Audit Manager et les gérer. En d'autres termes, en plus de désigner un utilisateur en tant que propriétaire de l'audit, vous devez également associer les politiques IAM nécessaires à cet utilisateur. L'idée sous-jacente est qu'en exigeant les deux, Audit Manager vous garantit un contrôle total sur toutes les spécificités de chaque évaluation.

> **Note**
>
> Pour les responsables de l'audit, nous vous recommandons d'utiliser cette AWSAuditManagerAdministratorAccesspolitique. Pour plus d'informations, consultez Politiques recommandées pour les personas utilisateurs dans AWS Audit Manager.

Je ne parviens pas à exécuter une action dans Audit Manager

Si vous ne disposez pas des autorisations nécessaires pour utiliser la AWS Audit Manager console ou les opérations de l'API Audit Manager, il est probable que vous rencontriez une `AccessDeniedException` erreur.

Pour résoudre ce problème, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations de connexion.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder aux ressources de mon Audit Manager

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Audit Manager prend en charge ces fonctionnalités, consultez Comment AWS Audit Manager fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.

- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Je vois un message d'erreur « Accès refusé » alors que je dispose des autorisations d'Audit Manager requises

Si votre compte fait partie d'une organisation, il est possible que l'`Access Denied`erreur soit due à une politique de contrôle des services (SPC). Les SCP sont des politiques utilisées pour gérer les autorisations d'une organisation. Lorsqu'un SCP est en place, il peut refuser des autorisations spécifiques à tous les comptes membres, y compris le compte d'administrateur délégué que vous utilisez dans Audit Manager.

Par exemple, si votre organisation a mis en place un SCP qui refuse les autorisations pour les API de AWS Control Catalog, vous ne pouvez pas consulter les ressources fournies par Control Catalog. Cela est vrai même si vous disposez par ailleurs des autorisations requises pour Audit Manager, telles que la AWSAuditManagerAdministratorAccesspolitique. Le SCP annule les autorisations de politique gérées en refusant explicitement l'accès aux API du catalogue de contrôle.

Voici un exemple d'un tel SCP. Une fois ce SCP en place, votre compte d'administrateur délégué n'a pas accès aux contrôles communs, aux objectifs de contrôle et aux domaines de contrôle nécessaires pour utiliser la fonctionnalité de contrôles communs d'Audit Manager.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "controlcatalog:ListCommonControls",
                "controlcatalog:ListObjectives",
                "controlcatalog:ListDomains",
            ],
            "Resource": "*"
        }
    ]
}
```

Pour résoudre ce problème, nous vous recommandons de suivre les étapes suivantes :

1. Vérifiez si un SCP est rattaché à votre organisation. Pour obtenir des instructions, consultez la section Obtenir des informations sur les politiques de votre organisation dans le guide de l'utilisateur d'AWS Organizations.
2. Identifiez si le SCP est à l'origine de l'`Access Denied`erreur.
3. Mettez à jour le SCP pour vous assurer que votre compte d'administrateur délégué dispose de l'accès nécessaire à Audit Manager. Pour obtenir des instructions, consultez la section Mettre à jour un SCP dans le guide de l'utilisateur d'AWS Organizations.

Ressources supplémentaires

Les pages suivantes contiennent des conseils pour la résolution d'autres problèmes pouvant être dus à des autorisations manquantes :

- Je ne vois aucun contrôle ou ensemble de contrôles dans mon évaluation
- L'option de règle personnalisée n'est pas disponible lorsque je configure une source de données pour un contrôle
- Je reçois un message d'erreur d'accès refusé lorsque j'essaie de générer un rapport
- Je reçois un message d'erreur accès refusé lorsque j'essaie de générer un rapport d'évaluation à l'aide de mon compte administrateur délégué
- Je ne parviens pas à activer l'outil de recherche d'éléments probants
- Je ne parviens pas à désactiver l'outil de recherche d'éléments probants
- Ma requête de recherche échoue
- J'ai spécifié une rubrique Amazon SNS dans Audit Manager, mais je ne reçois aucune notification

Ressources de balisage AWS Audit Manager

Une balise est une étiquette de métadonnées que vous attribuez ou que vous AWS attribuez à une AWS ressource. Chaque balise se compose d'une clé et d'une valeur. Pour les balises que vous affectez, vous définissez la clé et la valeur. Par exemple, vous pouvez définir la clé sur `stage` et la valeur pour une ressource sur `test`.

Les balises vous permettent d'effectuer les actions suivantes :

- Localisez facilement les ressources de votre Audit Manager. Vous pouvez utiliser des balises comme critères de recherche lorsque vous parcourez la bibliothèque du framework et la bibliothèque de contrôle.
- Associez votre ressource à un type de conformité. Vous pouvez étiqueter plusieurs ressources à l'aide d'une balise spécifique à la conformité afin d'associer ces ressources à un framework spécifique.
- Identifiez et organisez vos AWS ressources. Beaucoup Services AWS prennent en charge le balisage. Vous pouvez donc attribuer le même tag aux ressources provenant de différents services pour indiquer que les ressources sont liées.
- Suivez vos AWS coûts. Vous activez ces balises sur le AWS Billing and Cost Management tableau de bord. AWS utilise les balises pour classer vos coûts et vous fournir un rapport mensuel de répartition des coûts. Pour plus d'informations, consultez Utilisation des balises de répartition des coûts dans le Guide de l'utilisateur AWS Billing and Cost Management .

Les sections suivantes fournissent plus d'informations sur les balises pour AWS Audit Manager.

Table des matières

Ressources prises en charge dans Audit Manager

Les ressources Audit Manager suivantes prennent en charge le balisage :

- Évaluations

- Contrôles
- Frameworks

Restrictions liées aux balises

Les restrictions de base suivantes s'appliquent aux balises sur les ressources Audit Manager :

- Nombre maximum d'étiquettes que vous pouvez attribuer à une ressource – 50
- Longueur de clé maximale – 128 caractères Unicode
- Longueur de valeur maximale – 256 caractères Unicode
- Caractères valides pour les clés et valeurs – a-z, A-Z, 0-9, espace et les caractères suivants : _ . : / = + - et @
- Les clés et les valeurs sont sensibles à la casse.
- Ne l'utilisez pas `aws:` comme préfixe pour les clés ; il est réservé à l'usage AWS

Ressources supplémentaires

Vous pouvez définir des balises en tant que propriétés lorsque vous créez une évaluation, un cadre ou un contrôle. Vous pouvez ajouter, modifier et supprimer des balises via la console Audit Manager, le AWS Command Line Interface (AWS CLI) et l'API Audit Manager. Pour de plus amples informations, consultez les liens suivants.

- Pour le balisage des évaluations :
  - Création d'une évaluation dans AWS Audit Manager et Modifier une évaluation dans AWS Audit Manager dans la section Évaluations de ce guide
  - Onglet Balisesdans la page Réviser une évaluation de ce guide
  - CreateAssessmentet UpdateAssessmentdans la référence de AWS Audit Manager l'API
  - TagResourceet UntagResourcedans la référence de AWS Audit Manager l'API
- Pour les frameworks de balisage :
  - Création d'un framework personnalisé dans AWS Audit Manager et Modification d'un framework personnalisé dans AWS Audit Manager dans la section Bibliothèque Framework de ce guide
  - La Tags tab page de détails du framework View de ce guide
  - CreateAssessmentFrameworket UpdateAssessmentFrameworkdans la référence de AWS Audit Manager l'API

  - TagResourceet UntagResourcedans la référence de AWS Audit Manager l'API
- Pour les commandes de balisage :
  - Création d'un contrôle personnalisé dans AWS Audit Manager et Modification d'un contrôle personnalisé dans AWS Audit Manager dans la section Bibliothèque de contrôle de ce guide
  - La Tags section de la page Révision d'un contrôle personnalisé de ce guide
  - La Tags section de la page Révision d'un contrôle standard de ce guide
  - CreateControlet UpdateControldans la référence de AWS Audit Manager l'API
  - TagResourceet UntagResourcedans la référence de AWS Audit Manager l'API

Comprendre les quotas et les restrictions pour AWS Audit Manager

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chacun d'entre eux Service AWS. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés.

La plupart des quotas d'Audit Manager, mais pas tous, sont répertoriés sous l'espace de AWS Audit Manager noms de la console Service Quotas. Pour savoir comment demander une augmentation de quota, consultez Gestion de vos quotas d'Audit Manager.

Table des matières

Quotas par défaut d'Audit Manager

Les AWS Audit Manager quotas suivants sont établis Compte AWS par région.

Ressource	Quota
Évaluations	Nombre d'évaluations actives par compte : 100
Rapports d'évaluation	Nombre d'éléments probants que vous pouvez ajouter à un rapport d'évaluation : • Pour les rapports portant sur la même région (où l'évaluation et le compartiment S3 de destination du rapport d'évaluation se trouvent dans le même compartiment Région AWS) : 22 000 • Pour les rapports inter-région (où l'évaluation et le compartim ent S3 de destination du rapport d'évaluation se trouvent dans le même compartiment Régions AWS) : 3 500

Ressource	Quota
	• Pour les rapports où l'évaluation associée utilise un client géré AWS KMS key : 3 500
Contrôles	Nombre de tâches simultanées par compte : 500
Preuve	Taille maximale d'un seul fichier d'élément probant manuel : 100 Mo Nombre de téléchargements manuels quotidiens d'éléments probants par contrôle : 100 **Tip** Si vous devez télécharger un grand nombre d'élément s probants manuels vers un seul contrôle, nous vous recommandons de charger vos éléments probants par lots sur plusieurs jours.
Frameworks	Nombre de frameworks personnalisés par compte : 100 **Note** Les quotas de framework s'appliquent à tous les framework s personnalisés partagés de votre bibliothèque de frameworks, quelle que soit la personne ayant créé le framework.
Destinataires du framework personnalisé partagé	Nombre de comptes bénéficiaires actifs : 100
Accès à l'API	Nombre de transactions par seconde (TPS) sur toutes les API : 20 TPS

Gestion de vos quotas d'Audit Manager

AWS Audit Manager est intégré à Service Quotas et vous permet de consulter et de gérer vos quotas à partir d'un emplacement central. Service AWS Service Quotas facilite la recherche de la valeur de vos quotas d'Audit Manager.

Pour afficher Service Quotas d'Audit Manager à l'aide de la console

1. Ouvrez la console Service Quotas à l'adresse https://console.aws.amazon.com/servicequotas/.
2. Dans le panneau de navigation, sélectionnez Services AWS.
3. Dans la liste Services AWS, recherchez et sélectionnez AWS Audit Manager.
4. Dans la liste des quotas de service, vous pouvez voir le nom du quota de service, la valeur du quota appliqué (si elle est disponible), la valeur du quota AWS par défaut et si le quota est ajustable.
5. Pour afficher des informations supplémentaires sur un quota de service, notamment la description, choisissez le nom du quota.
6. (Facultatif) Pour demander une augmentation de quota, sélectionnez le quota que vous souhaitez augmenter, sélectionnez Request quota increase (Demander une augmentation de quota), saisissez ou sélectionnez les informations requises, puis sélectionnez Request (Demander).

Ressources supplémentaires

Pour plus d'informations sur la gestion de vos quotas, consultez la section Demander une augmentation de quota dans le Guide de l'utilisateur du Service Quotas.

Pour de plus amples informations sur les quotas de service, veuillez consulter Qu'est-ce que les quotas de service ? dans le Guide de l'utilisateur des quotas de service.

Comprendre la sécurité et la protection des données dans AWS Audit Manager

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui fonctionne Services AWS dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Audit Manager, voir AWS Services concernés par programme de conformitéAWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par Service AWS ce que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation AWS Audit Manager. Les rubriques suivantes expliquent comment configurer Audit Manager pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à en utiliser d'autres Services AWS qui vous aident à surveiller et à sécuriser les ressources de votre Audit Manager.

Rubriques

- Connexion et surveillance AWS Audit Manager
- Comprendre la configuration et l'analyse des vulnérabilités dans AWS Audit Manager

Protection des données dans AWS Audit Manager

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS Audit Manager. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Audit Manager ou un autre outil Services AWS à l'aide de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Outre la recommandation ci-dessus, nous recommandons spécifiquement aux clients d'Audit Manager de ne pas inclure d'informations d'identification sensibles dans les champs au format de texte libre lors de la création d'évaluations, de contrôles personnalisés, de cadres personnalisés et de commentaires de délégation.

Suppression des données d'Audit Manager

Les données d'Audit Manager peuvent être supprimées de plusieurs manières.

Suppression des données lors de la désactivation d'Audit Manager

Lorsque vous désactivez Audit Manager, vous pouvez décider si vous souhaitez supprimer toutes vos données d'Audit Manager. Si vous choisissez de supprimer vos données, elles seront supprimées dans les 7 jours suivant la désactivation d'Audit Manager. Une fois vos données supprimées, vous ne pouvez pas les récupérer.

Suppression automatique des données

Certaines données d'Audit Manager sont supprimées automatiquement après un certain temps. Audit Manager conserve les données des clients comme suit.

Type de données	Période de conservation des données	Remarques
Éléments probants	Les données sont conservées pendant 2 ans	Cela comprend les éléments probants automatisés et manuels

Type de données	Période de conservation des données	Remarques
	à partir de leur création	
Ressources créées par le client	Les données sont conservées indéfiniment	Cela comprend les évaluations, les rapports d'évaluation, les contrôles personnalisés et les frameworks personnalisés

Suppression manuelle des données

Vous pouvez supprimer des ressources d'Audit Manager à tout moment. Pour obtenir des instructions, veuillez consulter les sections suivantes :

- Supprimer une évaluation dans AWS Audit Manager
  - Voir également : DeleteAssessmentdans la référence de AWS Audit Manager l'API
- Suppression d'un framework personnalisé dans AWS Audit Manager
  - Voir également : DeleteAssessmentFrameworkdans la référence de AWS Audit Manager l'API
- Supprimer des demandes de partage dans AWS Audit Manager
  - Voir également : DeleteAssessmentFrameworkSharedans la référence de AWS Audit Manager l'API
- Suppression d'un rapport d'évaluation
  - Voir également : DeleteAssessmentReportdans la référence de AWS Audit Manager l'API
- Suppression d'un contrôle personnalisé dans AWS Audit Manager
  - Voir également : DeleteControldans la référence de AWS Audit Manager l'API

Pour supprimer d'autres éventuelles données de ressources créées lors de votre utilisation d'Audit Manager, consultez ce qui suit :

- Supprimer un entrepôt de données d'événements dans le Guide de l'utilisateur AWS CloudTrail
- Suppression d'un compartiment dans le Guide de l'utilisateur d'Amazon Simple Storage Service (Amazon S3).

Chiffrement au repos

Pour chiffrer les données au repos, Audit Manager utilise le chiffrement côté serveur Clés gérées par AWS pour tous ses magasins de données et ses journaux.

Vos données sont cryptées sous une clé gérée par le client ou un Clé détenue par AWS, selon les paramètres que vous avez sélectionnés. Si vous ne fournissez pas de clé gérée par le client, Audit Manager utilise un Clé détenue par AWS pour chiffrer votre contenu. Toutes les métadonnées de service dans DynamoDB et Amazon S3 dans Audit Manager sont chiffrées à l'aide d'une Clé détenue par AWS.

Audit Manager chiffre les données comme suit :

- Les métadonnées de service stockées dans Amazon S3 sont chiffrées dans le cadre d'un Clé détenue par AWS SSE-KMS.
- Les métadonnées de service stockées dans DynamoDB sont chiffrées côté serveur à l'aide de KMS et d'une Clé détenue par AWS.
- Votre contenu stocké dans DynamoDB est chiffré côté client à l'aide d'une clé gérée par le client ou d'une Clé détenue par AWS. La clé KMS est basée sur les paramètres que vous avez choisis.
- Votre contenu stocké dans Amazon S3 dans Audit Manager est chiffré à l'aide d'une clé SSE-KMS. La clé KMS dépend des paramètres sélectionnés et peut être une clé gérée par le client ou une Clé détenue par AWS.
- Les rapports d'évaluation publiés dans votre compartiment S3 sont chiffrés comme suit :
  - Si vous avez fourni une clé gérée par le client, vos données sont cryptées à l'aide de SSE-KMS.
  - Si vous avez utilisé le Clé détenue par AWS, vos données sont cryptées à l'aide du SSE-S3.

Chiffrement en transit

Audit Manager fournit des points de terminaison sécurisés et privés pour le chiffrement des données en transit. Les points de terminaison sécurisés et privés permettent AWS de protéger l'intégrité des demandes d'API adressées à Audit Manager.

Transit interservices

Par défaut, toutes les communications interservices sont protégées par un chiffrement utilisant le protocole TLS (Transport Layer Security).

Gestion des clés

Audit Manager prend en charge à la fois Clés détenues par AWS les clés gérées par le client pour chiffrer toutes les ressources d'Audit Manager (évaluations, contrôles, cadres, preuves et rapports d'évaluation enregistrés dans les compartiments S3 de vos comptes).

Nous vous recommandons d'utiliser une clé gérée par le client. Ce faisant, vous pouvez consulter et gérer les clés de chiffrement qui protègent vos données, y compris les journaux concernant leur utilisation dans AWS CloudTrail. Si vous choisissez une clé gérée par le client, Audit Manager crée une attribution sur la clé KMS, afin de pouvoir l'utiliser pour chiffrer votre contenu.

> **Warning**
>
> Après la suppression ou la désactivation d'une clé KMS utilisée pour chiffrer les ressources Audit Manager, vous ne pouvez plus déchiffrer les ressources chiffrées à l'aide de cette clé, ce qui signifie que les données deviennent irrécupérables.
> La suppression d'une clé KMS dans AWS Key Management Service (AWS KMS) est destructrice et potentiellement dangereuse. Pour plus d'informations sur la suppression des clés KMS, consultez la section Suppression AWS KMS keys du guide de l'utilisateur AWS Key Management Service .

Vous pouvez spécifier vos paramètres de chiffrement lorsque vous activez Audit Manager à l' AWS Management Console aide de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI). Pour obtenir des instructions, veuillez consulter Activant AWS Audit Manager.

Vous pouvez consulter et modifier vos paramètres de chiffrement à tout moment. Pour obtenir des instructions, veuillez consulter Configuration de vos paramètres de chiffrement des données.

Pour plus d'informations sur la configuration des clés gérées par le client, consultez la section Création de clés du guide de l'utilisateur AWS Key Management Service .

Gestion des identités et des accès pour AWS Audit Manager

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent les personnes qui peuvent être authentifiées (connectées) et autorisées (dotées

d'autorisations) à utiliser des ressources Audit Manager. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Audit Manager.

Utilisateur du service : si vous utilisez le service Audit Manager pour effectuer votre tâche, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Plus vous utiliserez de fonctionnalités Audit Manager pour effectuer votre travail, plus vous pourriez avoir besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans Audit Manager, veuillez consulter Résolution des problèmes AWS Audit Manager d'identité et d'accès.

Administrateur du service : si vous êtes le responsable des ressources Audit Manager de votre entreprise, vous bénéficiez probablement d'un accès complet à Audit Manager. Il est de votre responsabilité de déterminer les fonctionnalités et ressources Audit Manager auxquelles les utilisateurs de votre service doivent pouvoir accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec Audit Manager, veuillez consulter Comment AWS Audit Manager fonctionne avec IAM.

Administrateur IAM : si vous êtes un administrateur IAM, vous souhaiterez peut-être en savoir plus sur la création de politiques d'accès à Audit Manager. Pour voir des exemples de politiques Audit Manager basées sur l'identité que vous pouvez utiliser dans IAM, veuillez consulter Exemples de politiques basées sur l'identité pour AWS Audit Manager.

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès.

Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent

le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur IAM.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations,

consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment AWS Audit Manager fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Audit Manager, découvrez les fonctionnalités IAM que vous pouvez utiliser avec Audit Manager.

Fonctionnalités IAM que vous pouvez utiliser avec AWS Audit Manager

Fonction IAM	Prise en charge par Audit Manager
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d'une politique	Partielle
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Oui
Transmission des sessions d'accès (FAS)	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont AWS Audit Manager les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour AWS Audit Manager

Prend en charge les politiques basées sur l'identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles

ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

AWS Audit Manager crée une politique gérée nommée `AWSAuditManagerAdministratorAccess` pour les administrateurs d'Audit Manager. Cette politique accorde un accès administratif complet dans Audit Manager. Les administrateurs peuvent associer cette politique à n'importe quel rôle ou utilisateur existant, ou créer un nouveau rôle avec cette politique.

Politiques recommandées pour les personas utilisateurs dans AWS Audit Manager

AWS Audit Manager vous permet de maintenir la séparation des tâches entre les différents utilisateurs et pour les différents audits en utilisant différentes politiques IAM. Les deux personna dans Audit Manager et leurs politiques recommandées sont définies comme suit.

Persona	Description et politique recommandée
Responsable de l'audit	• Ce personnage doit disposer des autorisations nécessaires pour gérer les évaluations dans AWS Audit Manager. • La stratégie recommandée à utiliser pour ce personnage est la stratégie gérée nommée AWSAuditManagerAdministratorAccess. Vous pouvez utiliser cette politique comme point de départ et définir la portée de ces autorisations en fonction de vos besoins.
Délégué	• Cette persona peut accéder aux séries de contrôles déléguées dans le cadre d'une évaluation. Elle peut mettre à jour l'état du contrôle, ajouter des commentaires, soumettre une série de contrôles pour examen et ajouter des éléments probants au rapport d'évaluation. • La politique recommandée à utiliser pour cette persona est l'exemple de politique suivant : Autoriser l'accès de gestion des utilisateurs à AWS Audit Manager. Vous pouvez utiliser cette politique comme point de départ et apporter les modifications nécessaires en fonction de vos besoins.

Exemples de politiques basées sur l'identité pour AWS Audit Manager

Pour voir des exemples de politiques basées sur l'identité, consultez Exemples de politiques basées sur l'identité pour AWS Audit Manager.

Politiques basées sur les ressources au sein de AWS Audit Manager

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions politiques pour AWS Audit Manager

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des AWS Audit Manager actions, consultez la section Actions définies par AWS Audit Manager dans le Service Authorization Reference.

Les actions de politique en AWS Audit Manager cours utilisent le préfixe suivant avant l'action.

```
auditmanager
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "auditmanager:GetEvidenceDetails",
      "auditmanager:GetEvidenceEventDetails"
         ]
```

Vous pouvez aussi préciser plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Get`, incluez l'action suivante.

```
"Action": "auditmanager:Get*"
```

Pour voir des exemples de politiques basées sur l'identité, consultez Exemples de politiques basées sur l'identité pour AWS Audit Manager.

Ressources politiques pour AWS Audit Manager

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de AWS Audit Manager ressources et leurs ARN, consultez la section Ressources définies par AWS Audit Manager dans le Service Authorization Reference. Pour connaître les actions permettant de spécifier l'ARN de chaque ressource, consultez la section Actions définies par AWS Audit Manager.

Une évaluation Audit Manager possède le format d'Amazon Resource Name (ARN) suivant :

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

Une série de contrôles Audit Manager possède le format d'ARN suivant :

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/
${assessmentId}controlSet/${controlSetId}
```

Un contrôle Audit Manager possède le format d'ARN suivant :

```
arn:${Partition}:auditmanager:${Region}:${Account}:control/${controlId}
```

Pour de plus amples informations sur les formats d'ARN, veuillez consulter la section Amazon Ressource Names (ARN).

Par exemple, pour spécifier l'évaluation avec l'ID `i-1234567890abcdef0` dans votre instruction, utilisez l'ARN suivant.

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/
i-1234567890abcdef0"
```

Pour spécifier toutes les instances qui appartiennent à un compte spécifique, utilisez le caractère générique (*).

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/*"
```

Certaines actions Audit Manager, comme celles liées à la création de ressources, ne peuvent pas être exécutées sur une ressource précise. Dans ces cas-là, vous devez utiliser le caractère générique (*).

```
"Resource": "*"
```

De nombreuses actions de l'API Audit Manager impliquent plusieurs ressources. Par exemple, `ListAssessments` renvoie une liste de métadonnées d'évaluation accessibles aux personnes actuellement connectées Compte AWS. Par conséquent, un utilisateur doit être autorisé à consulter les évaluations. Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN par des virgules.

```
"Resource": [
      "resource1",
      "resource2"
```

Pour afficher une liste des types de ressources Audit Manager et de leurs ARN, veuillez consulter la section Ressources définies par AWS Audit Manager dans le Guide de l'utilisateur IAM. Pour connaître les actions permettant de spécifier l'ARN de chaque ressource, consultez la section Actions définies par AWS Audit Manager.

Certaines actions de l'API Audit Manager prennent en charge plusieurs ressources. Par exemple, `GetChangeLogs` accède à un `assessmentID`, un `controlID` et un `controlSetId`, donc un

principal doit posséder les autorisations nécessaires pour accéder à chacune de ces ressources. Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN par des virgules.

```
"Resource": [
      "assessmentId",
      "controlId",
      "controlSetId"
```

Clés de conditions de politique pour AWS Audit Manager

Prend en charge les clés de condition de politique spécifiques au service	Partielle

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Lorsque le principal d'une instruction de politique est un principal du service AWS, nous vous recommandons vivement d'utiliser les clés de condition globales `aws:SourceArn` ou `aws:SourceAccount` dans la politique. Vous pouvez utiliser ces clés contextuelles de condition globale pour éviter le scénario de l'adjoint désorienté. Les politiques documentées suivantes expliquent l'utilisation des clés contextuelles de condition globale `aws:SourceArn` et `aws:SourceAccount` dans Audit Manager afin d'éviter le problème de l'adjoint désorienté.

- Exemple de politique pour une rubrique SNS utilisée pour les notifications d'Audit Manager
- Exemple de politique de clé KMS utilisée avec une rubrique SNS

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur. Pour plus d'informations, consultez la section Éléments d'une politique IAM : variables et balises dans le Guide de l'utilisateur IAM.

Audit Manager ne fournit pas de clés de condition spécifiques au service, mais prend en charge l'utilisation de certaines clés de condition globales. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Listes de contrôle d'accès (ACL) dans AWS Audit Manager

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Contrôle d'accès basé sur les attributs (ABAC) avec AWS Audit Manager

Prend en charge ABAC (étiquettes dans les politiques)	Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur le balisage AWS Audit Manager des ressources, consultezRessources de balisage AWS Audit Manager.

Utilisation d'informations d'identification temporaires avec AWS Audit Manager

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Transférer les sessions d'accès pour AWS Audit Manager

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Fonctions du service pour AWS Audit Manager

Prend en charge les fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations d'une fonction du service peut altérer la fonctionnalité d' AWS Audit Manager . Ne modifiez des fonctions de service que lorsqu'Amazon ECS vous le conseille.

Rôles liés à un service pour AWS Audit Manager

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus de détails sur les rôles liés à un service pour AWS Audit Manager, consultez. Utilisation de rôles liés à un service pour AWS Audit Manager

Exemples de politiques basées sur l'identité pour AWS Audit Manager

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier des ressources Audit Manager. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par AWS Audit Manager, y compris le format des ARN pour chacun des types de ressources, veuillez consulter Actions, ressources et clés de condition pour AWS Audit Manager dans la Référence de l'autorisation de service.

Table des matières

- Autoriser les utilisateurs à accéder en lecture seule à AWS Audit Manager
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- AWS Audit Manager Autoriser l'envoi de notifications aux rubriques Amazon SNS
  - Exemple 1 (Autorisations pour la rubrique SNS)
  - Exemple 2 (autorisations pour la clé KMS associée à la rubrique SNS)
- Autoriser les utilisateurs à exécuter des requêtes de recherche dans l'outil de recherche d'éléments probants

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources Audit Manager dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Ajoutez les autorisations minimales requises pour activer Audit Manager

Cet exemple montre comment autoriser des comptes sans rôle d'administrateur à activer AWS Audit Manager.

> **Note**
>
> Ce que nous proposons ici est une politique de base accordant les autorisations minimales nécessaires pour activer Audit Manager. Toutes les autorisations définies dans la politique suivante sont requises. Si vous omettez une partie de cette politique, vous ne pourrez pas activer Audit Manager.
> Nous vous recommandons de prendre le temps de personnaliser vos autorisations en fonction de vos besoins spécifiques. Si vous avez encore besoin d'aide, contactez votre administrateur ou AWS Support.

Pour accorder l'accès minimum requis pour activer Audit Manager, utilisez les autorisations suivantes.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": "auditmanager:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                   ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Effect": "Allow",
            "Action": "kms:ListAliases",
            "Resource": "*",
            "Condition": {
```

```
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        }
    ]
}
```

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API que vous tentez d'effectuer.

Permettre aux utilisateurs un accès administrateur complet à AWS Audit Manager

Les exemples de politiques suivants accordent un accès administrateur complet à AWS Audit Manager.

- Exemple 1 (politique gérée, `AWSAuditManagerAdministratorAccess`)
- Exemple 2 (autorisations de destination du rapport d'évaluation)
- Exemple 3 (autorisations de destination d'exportation)
- Exemple 4 (Autorisations pour activer l'outil de recherche d'éléments probants)
- Exemple 5 (Autorisations pour désactiver l'outil de recherche d'éléments probants)

Exemple 1 (politique gérée, **`AWSAuditManagerAdministratorAccess`**)

La AWSAuditManagerAdministratorAccesspolitique inclut la possibilité d'activer et de désactiver Audit Manager, la possibilité de modifier les paramètres d'Audit Manager et la capacité de gérer toutes les ressources d'Audit Manager telles que les évaluations, les cadres, les contrôles et les rapports d'évaluation.

Exemple 2 (autorisations de destination du rapport d'évaluation)

Cette politique vous autorise à accéder à un compartiment S3 spécifique, à y ajouter des fichiers et à en supprimer. Cela vous permet d'utiliser le compartiment spécifié comme destination du rapport d'évaluation dans Audit Manager.

Remplacez chaque *`espace réservé`* par vos propres informations. Incluez le compartiment S3 destination de votre rapport d'évaluation et la clé KMS utilisée pour chiffrer vos rapports d'évaluation.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "s3:PutObject",
               "s3:GetObject",
               "s3:ListBucket",
               "s3:DeleteObject",
               "s3:GetBucketLocation",
               "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
        }
    ]
},
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

Exemple 3 (autorisations de destination d'exportation)

La politique suivante permet de CloudTrail fournir les résultats des requêtes Evidence Finder au compartiment S3 spécifié. En tant que bonne pratique en matière de sécurité, la clé de condition globale IAM `aws:SourceArn` permet de garantir que les CloudTrail écritures dans le compartiment S3 ne sont destinées qu'au magasin de données d'événements.

Remplacez *l'espace réservé* par vos propres informations.

- Remplacez DOC-EXAMPLE-DESTINATION-BUCKET par le compartiment S3 utilisé comme destination d'exportation.

- Remplacez *myQueryRunningRegion* par la région appropriée Région AWS à votre configuration.
- Remplacez *MyAccountID* par l' Compte AWS ID utilisé pour. CloudTrail Il se peut qu'il ne soit pas identique à l'ID Compte AWS du compartiment S3. S'il s'agit d'un magasin de données sur les événements d'une organisation, vous devez utiliser le Compte AWS pour le compte de gestion.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemple 4 (Autorisations pour activer l'outil de recherche d'éléments probants)

La politique d'autorisation suivante est requise si vous souhaitez activer et utiliser la fonctionnalité de recherche d'éléments probants. Cette déclaration de politique permet à Audit Manager de créer un magasin de données d'événements CloudTrail Lake et d'exécuter des requêtes de recherche.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
           "Sid": "ManageCloudTrailLakeQueryAccess",
           "Effect": "Allow",
           "Action": [
               "cloudtrail:StartQuery",
               "cloudtrail:DescribeQuery",
               "cloudtrail:GetQueryResults",
               "cloudtrail:CancelQuery"
           ],
```

```
            "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
        },
        {
            "Sid": "ManageCloudTrailLakeAccess",
            "Effect": "Allow",
            "Action": [
                 "cloudtrail:CreateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
         }
    ]
}
```

Exemple 5 (Autorisations pour désactiver l'outil de recherche d'éléments probants)

Cet exemple de politique autorise la désactivation de la fonctionnalité de recherche d'éléments probants dans Audit Manager. Cela implique de supprimer l'entrepôt de données d'événements créé lors de la première activation de cette fonctionnalité.

Pour utiliser cette politique, remplacez le *texte de l'espace réservé* par vos propres informations. Vous devez spécifier l'UUID de l'entrepôt de données d'événements créé lors de l'activation de l'outil de recherche d'éléments probants. Vous pouvez récupérer l'ARN de l'entrepôt de données d'événements à partir de vos paramètres Audit Manager. Pour plus d'informations, consultez GetSettingsla référence de AWS Audit Manager l'API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "cloudtrail:DeleteEventDataStore",
               "cloudtrail:UpdateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:::event-data-store-UUID"
        }
    ]
}
```

Autoriser l'accès de gestion des utilisateurs à AWS Audit Manager

Cet exemple montre comment autoriser un accès de gestion non administrateur à AWS Audit Manager.

Cette politique permet de gérer toutes les ressources d'Audit Manager (évaluations, frameworks et contrôles), mais ne permet pas d'activer ou de désactiver Audit Manager ou de modifier les paramètres d'Audit Manager.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:AssociateAssessmentReportEvidenceFolder",
                "auditmanager:BatchAssociateAssessmentReportEvidence",
                "auditmanager:BatchCreateDelegationByAssessment",
                "auditmanager:BatchDeleteDelegationByAssessment",
                "auditmanager:BatchDisassociateAssessmentReportEvidence",
                "auditmanager:BatchImportEvidenceToAssessmentControl",
                "auditmanager:CreateAssessment",
                "auditmanager:CreateAssessmentFramework",
                "auditmanager:CreateAssessmentReport",
                "auditmanager:CreateControl",
                "auditmanager:DeleteControl",
                "auditmanager:DeleteAssessment",
                "auditmanager:DeleteAssessmentFramework",
                "auditmanager:DeleteAssessmentFrameworkShare",
                "auditmanager:DeleteAssessmentReport",
                "auditmanager:DisassociateAssessmentReportEvidenceFolder",
                "auditmanager:GetAccountStatus",
                "auditmanager:GetAssessment",
                "auditmanager:GetAssessmentFramework",
                "auditmanager:GetControl",
                "auditmanager:GetServicesInScope",
                "auditmanager:GetSettings",
                "auditmanager:GetAssessmentReportUrl",
                "auditmanager:GetChangeLogs",
                "auditmanager:GetDelegations",
                "auditmanager:GetEvidence",
                "auditmanager:GetEvidenceByEvidenceFolder",
```

```
                "auditmanager:GetEvidenceFileUploadUrl",
                "auditmanager:GetEvidenceFolder",
                "auditmanager:GetEvidenceFoldersByAssessment",
                "auditmanager:GetEvidenceFoldersByAssessmentControl",
                "auditmanager:GetInsights",
                "auditmanager:GetInsightsByAssessment",
                "auditmanager:GetOrganizationAdminAccount",
                "auditmanager:ListAssessments",
                "auditmanager:ListAssessmentReports",
                "auditmanager:ListControls",
                "auditmanager:ListKeywordsForDataSource",
                "auditmanager:ListNotifications",
                "auditmanager:ListAssessmentControlInsightsByControlDomain",
                "auditmanager:ListAssessmentFrameworks",
                "auditmanager:ListAssessmentFrameworkShareRequests",
                "auditmanager:ListControlDomainInsights",
                "auditmanager:ListControlDomainInsightsByAssessment",
                "auditmanager:ListControlInsightsByControlDomain",
                "auditmanager:ListTagsForResource",
                "auditmanager:StartAssessmentFrameworkShare",
                "auditmanager:TagResource",
                "auditmanager:UntagResource",
                "auditmanager:UpdateControl",
                "auditmanager:UpdateAssessment",
                "auditmanager:UpdateAssessmentControl",
                "auditmanager:UpdateAssessmentControlSetStatus",
                "auditmanager:UpdateAssessmentFramework",
                "auditmanager:UpdateAssessmentFrameworkShare",
                "auditmanager:UpdateAssessmentStatus",
                "auditmanager:ValidateAssessmentReportIntegrity"
            ],
            "Resource": "*"
        },
        {
    "Sid": "ControlCatalogAccess",
    "Effect": "Allow",
    "Action": [
"controlcatalog:ListCommonControls",
"controlcatalog:ListDomains",
"controlcatalog:ListObjectives"
    ],
    "Resource": "*"
        },
        {
```

```
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
```

```
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Autoriser les utilisateurs à accéder en lecture seule à AWS Audit Manager

Cette politique accorde un accès en lecture seule aux AWS Audit Manager ressources telles que les évaluations, les cadres et les contrôles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:Get*",
                "auditmanager:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Audit Manager Autoriser l'envoi de notifications aux rubriques Amazon SNS

Les politiques de cet exemple accordent à Audit Manager l'autorisation d'envoyer des notifications à une rubrique Amazon SNS existante.

- Exemple 1 — Si vous souhaitez recevoir des notifications d'Audit Manager, utilisez cet exemple pour ajouter des autorisations à votre politique d'accès aux rubriques SNS.

- Exemple 2 — Si votre rubrique SNS utilise AWS Key Management Service (AWS KMS) pour le chiffrement côté serveur (SSE), utilisez cet exemple pour ajouter des autorisations à la politique d'accès aux clés KMS.

Dans les politiques suivantes, le principal qui obtient les autorisations est le principal du service Audit Manager, qui est `auditmanager.amazonaws.com`. Lorsque le principal d'une instruction de politique est un principal du service AWS, nous vous recommandons vivement d'utiliser les clés de condition globales `aws:SourceArn` ou `aws:SourceAccount` dans la politique. Vous pouvez utiliser ces clés contextuelles de condition globale pour éviter le scénario de l'adjoint désorienté.

Exemple 1 (Autorisations pour la rubrique SNS)

Cette instruction de politique autorise Audit Manager à publier des événements sur la rubrique SNS spécifiée. Toute demande de publication sur la rubrique SNS spécifiée doit satisfaire aux conditions de la politique.

Pour utiliser cette politique, remplacez le *`texte de l'espace réservé`* par vos propres informations. Notez les informations suivantes :

- Si vous utilisez la clé de condition `aws:SourceArn` dans cette politique, la valeur doit être l'ARN de la ressource Audit Manager d'où provient la notification. Dans l'exemple ci-dessous, `aws:SourceArn` utilise un caractère générique (`*`) pour l'ID de ressource. Cela autorise toutes les demandes provenant d'Audit Manager sur toutes les ressources d'Audit Manager. Avec la clé de condition globale `aws:SourceArn`, vous pouvez utiliser l'opérateur de condition `StringLike` ou `ArnLike`. Comme bonne pratique, nous vous recommandons d'utiliser `ArnLike`.
- Avec la clé de condition `aws:SourceAccount`, vous pouvez utiliser l'opérateur de condition `StringEquals` ou `StringLike`. Comme bonne pratique, nous vous recommandons d'utiliser `StringEquals` pour la mise en place du moindre privilège.
- Si vous utilisez à la fois `aws:SourceAccount` et`aws:SourceArn`, les valeurs de compte doivent comporter le même ID de compte.

```
{
  "Version": "2012-10-17",
  "Statement": {
      "Sid": "AllowAuditManagerToUseSNSTopic",
      "Effect": "Allow",
      "Principal": {
        "Service": "auditmanager.amazonaws.com"
```

```
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:accountID:topicName",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountID"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
    }
}
```

L'exemple alternatif suivant utilise uniquement la clé de condition `aws:SourceArn`, avec l'opérateur de condition `StringLike` :

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
```

L'exemple alternatif suivant utilise uniquement la clé de condition `aws:SourceAccount`, avec l'opérateur de condition `StringLike` :

```
   "Condition": {
     "StringLike": {
       "aws:SourceAccount": "accountID"
     }
    }
```

Exemple 2 (autorisations pour la clé KMS associée à la rubrique SNS)

L'instruction de politique permet à Audit Manager d'utiliser la clé KMS pour générer la clé de donnéesutilisée pour chiffrer une rubrique SNS. Toute demande d'utilisation de la clé KMS pour l'opération spécifiée doit répondre aux conditions de la politique.

Pour utiliser cette politique, remplacez le *texte de l'espace réservé* par vos propres informations. Notez les informations suivantes :

- Si vous utilisez la clé de condition `aws:SourceArn` dans cette politique, la valeur doit être l'ARN de la ressource chiffrée. Par exemple, dans ce cas, il s'agit de la rubrique SNS de votre compte. Définissez la valeur sur l'ARN ou un modèle d'ARN avec des caractères génériques (*). Avec la clé de condition `aws:SourceArn`, vous pouvez utiliser l'opérateur de condition `StringLike` ou `ArnLike`. Comme bonne pratique, nous vous recommandons d'utiliser `ArnLike`.
- Avec la clé de condition `aws:SourceAccount`, vous pouvez utiliser l'opérateur de condition `StringEquals` ou `StringLike`. Comme bonne pratique, nous vous recommandons d'utiliser `StringEquals` pour la mise en place du moindre privilège. Si vous ne connaissez pas l'ARN de la rubrique SNS, vous pouvez utiliser `aws:SourceAccount`.
- Si vous utilisez à la fois `aws:SourceAccount` et`aws:SourceArn`, les valeurs de compte doivent comporter le même ID de compte.

```
{
     "Version": "2012-10-17",
     "Statement": {
       "Sid": "AllowAuditManagerToUseKMSKey",
       "Effect": "Allow",
       "Principal": {
           "Service": "auditmanager.amazonaws.com"
       },
       "Action": [
           "kms:Decrypt",
           "kms:GenerateDataKey"
       ],
       "Resource": "arn:aws:kms:region:accountID:key/*",
       "Condition": {
           "StringEquals": {
                "aws:SourceAccount": "accountID"
            }
            "ArnLike": {
                 "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
            }
      }
    }
  ]
}
```

L'exemple alternatif suivant utilise uniquement la clé de condition `aws:SourceArn`, avec l'opérateur de condition `StringLike` :

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
        }
      }
```

L'exemple alternatif suivant utilise uniquement la clé de condition `aws:SourceAccount`, avec l'opérateur de condition `StringLike` :

```
   "Condition": {
     "StringLike": {
       "aws:SourceAccount": "accountID"
     }
    }
```

Autoriser les utilisateurs à exécuter des requêtes de recherche dans l'outil de recherche d'éléments probants

La politique suivante accorde des autorisations pour effectuer des requêtes sur un magasin de données d'événements CloudTrail Lake. La politique d'autorisation est requise si vous souhaitez utiliser la fonctionnalité de recherche d'éléments probants.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageCloudTrailLakeQueryAccess",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "*"
        }
    ]
}
```

Prévention du cas de figure de l'adjoint désorienté entre services

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. En AWS, l'usurpation d'identité interservices peut entraîner un problème de confusion chez les adjoints. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé pour utiliser ses autorisations pour agir sur les ressources d'un autre client, lorsqu'il n'a pas l'autorisation de le faire. Pour éviter cela, Amazon Web Services fournit des outils qui peuvent vous aider à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous recommandons d'utiliser les clés contextuelles de condition `aws:SourceAccount`globale `aws:SourceArn`et les clés contextuelles dans les politiques de ressources afin de limiter les autorisations accordées à un autre service pour accéder à vos ressources. AWS Audit Manager

- Utilisez `aws:SourceArn` si vous souhaitez qu'une seule ressource soit associée à l'accès entre services. Vous pouvez également utiliser `aws:SourceArn` avec un caractère générique (`*`) si vous souhaitez spécifier plusieurs ressources.

  Par exemple, vous pouvez utiliser une rubrique Amazon SNS pour recevoir des notifications d'activité de la part d'Audit Manager. Dans ce cas, dans votre stratégie d'accès à la rubrique SNS, la valeur ARN de `aws:SourceArn` est la ressource Audit Manager d'où provient la notification. Comme il est probable que vous disposiez de plusieurs ressources Audit Manager, nous vous recommandons d'utiliser `aws:SourceArn` avec un caractère générique. Cela vous permet de spécifier toutes les ressources Audit Manager dans votre stratégie d'accès à la rubrique SNS.
- Utilisez `aws:SourceAccount` si vous souhaitez autoriser l'association d'une ressource de ce compte à l'utilisation interservices.
- Si la valeur `aws:SourceArn` ne contient pas l'ID de compte, tel qu'un ARN de compartiment Amazon S3, vous devez utiliser les deux clés de contexte de condition globale pour limiter les autorisations.
- Si vous utilisez les deux conditions et que la valeur de `aws:SourceArn` contient l'ID de compte, la valeur de `aws:SourceAccount` et le compte indiqué dans la valeur de `aws:SourceArn` doivent utiliser le même ID de compte lorsqu'il est utilisé dans la même déclaration de politique.
- Le moyen le plus efficace de se protéger du problème de l'adjoint désorienté consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource.

Si vous ne connaissez pas l'Amazon Resource Name (ARN) complet de la ressource ou spécifiez plusieurs ressources, utilisez la clé de contexte de condition globale `aws:SourceArn` avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:servicename:*:123456789012:*`.

Audit Manager : assistance adjoint désorienté

Audit Manager fournit une assistance adjoint désorienté dans les scénarios suivants. L'exemple suivant montre comment utiliser les clés de condition `aws:SourceArn` et `aws:SourceAccount` afin d'éviter le problème de l'adjoint désorienté.

- Exemple de politique : rubrique SNS utilisée pour recevoir les notifications d'Audit Manager
- Exemple de politique : clé KMS utilisée pour chiffrer votre rubrique SNS

Audit Manager ne fournit pas d'assistance adjoint désorienté pour la clé gérée par le client fournie dans vos paramètres Configuration de vos paramètres de chiffrement des données Audit Manager. Si vous avez fourni votre propre clé gérée par le client, vous ne pouvez pas utiliser les conditions `aws:SourceAccount` ou `aws:SourceArn` énoncées dans cette stratégie de clé KMS.

AWS politiques gérées pour AWS Audit Manager

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Rubriques

AWS politique gérée : AWSAuditManagerAdministratorAccess

Vous pouvez associer la politique `AWSAuditManagerAdministratorAccess` à vos identités IAM.

Cette politique accorde des autorisations administratives qui permettent un accès administratif complet à AWS Audit Manager. Cet accès inclut la possibilité d'activer et de désactiver AWS Audit Manager, de modifier les paramètres et de gérer toutes les ressources d'Audit Manager, telles que les évaluations, les cadres, les contrôles et les rapports d'évaluation. AWS Audit Manager

AWS Audit Manager nécessite des autorisations étendues pour plusieurs AWS services. Cela est dû au fait qu'il AWS Audit Manager s'intègre à plusieurs AWS services pour collecter automatiquement Compte AWS des preuves à partir des services concernés par une évaluation.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `Audit Manager` – Permet aux principaux d'obtenir des autorisations complètes sur les ressources AWS Audit Manager .
- `Organizations` – Permet aux principaux de répertorier les comptes et les unités organisationnelles, et d'enregistrer ou de désenregistrer un administrateur délégué. Cela est nécessaire pour que vous puissiez activer le support multi-comptes, AWS Audit Manager effectuer des évaluations sur plusieurs comptes et consolider les preuves dans un compte d'administrateur délégué.
- `iam` – Permet aux principaux d'obtenir et de répertorier les utilisateurs dans IAM et de créer un rôle lié à un service. Ceci est nécessaire pour pouvoir désigner les responsables d'audit et les délégués pour une évaluation. Cette politique autorise également les principaux à supprimer le rôle lié à un service et à récupérer l'état de suppression. Cela est nécessaire pour nettoyer les ressources et supprimer le rôle lié au service pour vous lorsque vous choisissez de désactiver le service dans le. AWS Audit Manager AWS Management Console

- `s3` – Permet aux principaux de répertorier les compartiments Amazon Simple Storage Service (Amazon S3) disponibles. Cette fonctionnalité est requise pour désigner le compartiment S3 dans lequel vous souhaitez stocker les rapports d'éléments probants ou télécharger les éléments probants manuels.
- `kms` – Permet aux principaux de répertorier et de décrire les clés, de répertorier les alias et de créer des attributions. Ceci est nécessaire pour choisir des clés gérées par le client pour le chiffrement des données.
- `sns` – Permet aux principaux de répertorier les rubriques d'abonnement dans Amazon SNS. Ceci est nécessaire pour spécifier la rubrique SNS à laquelle vous souhaitez que AWS Audit Manager envoie des notifications.
- `events`— Permet aux principaux de répertorier et de gérer les chèques provenant de AWS Security Hub. Cela est nécessaire pour AWS Audit Manager pouvoir collecter automatiquement AWS Security Hub les résultats des AWS services surveillés par AWS Security Hub. Il peut ensuite convertir ces données en éléments probants à inclure dans vos évaluations AWS Audit Manager .
- `tag` – Permet aux principaux de récupérer les ressources étiquetées. Ceci est nécessaire pour que vous puissiez utiliser les balises comme filtre de recherche lorsque vous parcourez les frameworks, les contrôles et les évaluations dans AWS Audit Manager.
- `controlcatalog`— Permet aux principaux de répertorier les domaines, les objectifs et les contrôles courants fournis par AWS Control Catalog. Cela est nécessaire pour que vous puissiez utiliser la fonction de commandes communes dans AWS Audit Manager. Une fois ces autorisations en place, vous pouvez consulter la liste des contrôles courants dans la bibliothèque de AWS Audit Manager contrôles et filtrer les contrôles par domaine et par objectif. Vous pouvez également utiliser des contrôles courants comme source de preuves lorsque vous créez un contrôle personnalisé.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
```

```
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
```

```
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
```

```
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
     "Sid": "ControlCatalogAccess",
     "Effect": "Allow",
     "Action": [
  "controlcatalog:ListCommonControls",
  "controlcatalog:ListDomains",
  "controlcatalog:ListObjectives"
     ],
     "Resource": "*"
        }
    ]
}
```

AWS politique gérée : AWSAuditManagerServiceRolePolicy

Vous ne pouvez pas joindre de `AWSAuditManagerServiceRolePolicy` à vos entités IAM. Cette politique est associée à un rôle lié à un service`AWSServiceRoleForAuditManager`, qui permet d' AWS Audit Manager effectuer des actions en votre nom. Pour plus d'informations, consultez Utilisation de rôles liés à un service pour AWS Audit Manager.

La politique d'autorisation des rôles, `AWSAuditManagerServiceRolePolicy`, permet à AWS Audit Manager de rassembler des éléments probants de manière automatisée en effectuant les opérations suivantes en votre nom :

- Rassembler des données à partir des sources de données suivantes :
  - Événements de gestion de AWS CloudTrail
  - Contrôles de conformité effectués par AWS Config Rules

  - Contrôles de conformité effectués par AWS Security Hub
- Utilisez les appels d'API pour décrire les configurations de vos ressources dans les Services AWS suivants.

> **Tip**
>
> Pour plus d'informations sur les appels d'API utilisés par Audit Manager pour rassembler des éléments probants provenant de ces services, consultez la section Appels d'API pris en charge pour les sources de données de contrôle personnalisées dans ce guide.

  - Amazon API Gateway
  - AWS Backup
  - Amazon Bedrock
  - AWS Certificate Manager
  - Amazon CloudFront
  - AWS CloudTrail
  - Amazon CloudWatch
  - Amazon CloudWatch Logs
  - Groupes d'utilisateurs Amazon Cognito
  - AWS Config
  - Amazon Data Firehose
  - AWS Direct Connect
  - Amazon DynamoDB
  - Amazon EC2
  - Amazon EC2 Auto Scaling
  - Amazon Elastic Container Service
  - Amazon Elastic File System
  - Amazon Elastic Kubernetes Service
  - Amazon ElastiCache
  - Elastic Load Balancing
  - Amazon EMR

- Amazon EventBridge
- Amazon FSx
- Amazon GuardDuty
- AWS Identity and Access Management (JE SUIS)
- Amazon Kinesis
- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Managed Streaming for Apache Kafka
- Amazon OpenSearch Service
- AWS Organizations
- Amazon Relational Database Service
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- Amazon SageMaker
- AWS Secrets Manager
- AWS Security Hub
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS WAF

Détails de l'autorisation

`AWSAuditManagerServiceRolePolicy`permet AWS Audit Manager de réaliser les actions suivantes sur les ressources spécifiées :

- `acm:GetAccountConfiguration`
- `acm:ListCertificates`
- `apigateway:GET`
- `autoscaling:DescribeAutoScalingGroups`
- `backup:ListBackupPlans`

- backup:ListRecoveryPointsByResource
- bedrock:GetCustomModel
- bedrock:GetFoundationModel
- bedrock:GetModelCustomizationJob
- bedrock:GetModelInvocationLoggingConfiguration
- bedrock:ListCustomModels
- bedrock:ListFoundationModels
- bedrock:ListModelCustomizationJobs
- cloudfront:GetDistribution
- cloudfront:GetDistributionConfig
- cloudfront:ListDistributions
- cloudtrail:DescribeTrails
- cloudtrail:GetTrail
- cloudtrail:ListTrails
- cloudtrail:LookupEvents
- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeBackup
- dynamodb:DescribeContinuousBackups
- dynamodb:DescribeTable
- dynamodb:DescribeTableReplicaAutoScaling
- dynamodb:ListBackups

- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstanceCreditSpecifications
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSecurityGroupRules
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointConnections
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault

- ec2:GetLaunchTemplateData
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- es:DescribeDomains
- es:DescribeDomain
- es:DescribeDomainConfig
- es:ListDomainNames
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems

- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccessKeyLastUsed
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:GetGroupPolicy
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:GetRolePolicy
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAccessKeys
- iam:ListAttachedGroupPolicies
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListEntitiesForPolicy
- iam:ListGroupsForUser
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListMfaDeviceTags
- iam:ListMfaDevices
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListPolicyVersions
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies

- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- logs:GetDataProtectionPolicy
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDBClusterEndpoints
- rds:DescribeDBClusterParameterGroups
- rds:DescribeDBClusters
- rds:DescribeDBInstances
- rds:DescribeDBInstanceAutomatedBackups

- rds:DescribeDBSecurityGroups
- redshift:DescribeClusters
- redshift:DescribeClusterSnapshots
- redshift:DescribeLoggingStatus
- route53:GetQueryLoggingConfig
- s3:GetBucketAcl
- s3:GetBucketLogging
- s3:GetBucketOwnershipControls
- s3:GetBucketPolicy
  - Cette action d'API fonctionne dans le cadre de l' Compte AWS endroit où elle service-linked-role est disponible. Elle ne peut pas accéder aux politiques de compartiments intercompte.
- s3:GetBucketPublicAccessBlock
- s3:GetBucketTagging
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- sagemaker:DescribeAlgorithm
- sagemaker:DescribeDomain
- sagemaker:DescribeEndpoint
- sagemaker:DescribeEndpointConfig
- sagemaker:DescribeFlowDefinition
- sagemaker:DescribeHumanTaskUi
- sagemaker:DescribeLabelingJob
- sagemaker:DescribeModel
- sagemaker:DescribeModelBiasJobDefinition
- sagemaker:DescribeModelCard
- sagemaker:DescribeModelQualityJobDefinition
- sagemaker:DescribeTrainingJob
- sagemaker:DescribeUserProfile

- sagemaker:ListAlgorithms
- sagemaker:ListDomains
- sagemaker:ListEndpointConfigs
- sagemaker:ListEndpoints
- sagemaker:ListFlowDefinitions
- sagemaker:ListHumanTaskUis
- sagemaker:ListLabelingJobs
- sagemaker:ListModels
- sagemaker:ListModelBiasJobDefinitions
- sagemaker:ListModelCards
- sagemaker:ListModelQualityJobDefinitions
- sagemaker:ListMonitoringAlerts
- sagemaker:ListMonitoringSchedules
- sagemaker:ListTrainingJobs
- sagemaker:ListUserProfiles
- securityhub:DescribeStandards
- secretsmanager:DescribeSecret
- secretsmanager:ListSecrets
- sns:ListTagsForResource
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:GetRule
- waf-regional:GetWebAcl
- waf-regional:ListRuleGroups
- waf-regional:ListRules
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:GetRule
- waf:GetRuleGroup

- waf:ListActivatedRulesInRuleGroup
- waf:ListRuleGroups
- waf:ListRules
- waf:ListWebAcls
- wafv2:ListWebAcls

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "acm:GetAccountConfiguration",
    "acm:ListCertificates",
    "autoscaling:DescribeAutoScalingGroups",
    "backup:ListBackupPlans",
    "backup:ListRecoveryPointsByResource",
    "bedrock:GetCustomModel",
    "bedrock:GetFoundationModel",
    "bedrock:GetModelCustomizationJob",
    "bedrock:GetModelInvocationLoggingConfiguration",
    "bedrock:ListCustomModels",
    "bedrock:ListFoundationModels",
    "bedrock:ListModelCustomizationJobs",
    "cloudfront:GetDistribution",
    "cloudfront:GetDistributionConfig",
    "cloudfront:ListDistributions",
    "cloudtrail:GetTrail",
    "cloudtrail:ListTrails",
    "cloudtrail:DescribeTrails",
    "cloudtrail:LookupEvents",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:DescribeAlarmsForMetric",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cognito-idp:DescribeUserPool",
    "config:DescribeConfigRules",
    "config:DescribeDeliveryChannels",
    "config:ListDiscoveredResources",
    "directconnect:DescribeDirectConnectGateways",
    "directconnect:DescribeVirtualGateways",
```

```
    "dynamodb:DescribeContinuousBackups",
    "dynamodb:DescribeBackup",
    "dynamodb:DescribeTableReplicaAutoScaling",
    "dynamodb:DescribeTable",
    "dynamodb:ListBackups",
    "dynamodb:ListGlobalTables",
    "dynamodb:ListTables",
    "ec2:DescribeInstanceCreditSpecifications",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeSecurityGroupRules",
    "ec2:DescribeVpcEndpointConnections",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:GetLaunchTemplateData",
    "ec2:DescribeAddresses",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeFlowLogs",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
    "ec2:DescribeLocalGateways",
    "ec2:DescribeLocalGatewayVirtualInterfaces",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:GetEbsEncryptionByDefault",
    "ecs:DescribeClusters",
    "eks:DescribeAddonVersions",
    "elasticache:DescribeCacheClusters",
    "elasticache:DescribeServiceUpdates",
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeFileSystems",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeSslPolicies",
```

```
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticmapreduce:ListClusters",
    "elasticmapreduce:ListSecurityConfigurations",
    "events:DescribeRule",
    "events:ListConnections",
    "events:ListEventBuses",
    "events:ListEventSources",
    "events:ListRules",
    "firehose:ListDeliveryStreams",
    "fsx:DescribeFileSystems",
    "guardduty:ListDetectors",
    "iam:GenerateCredentialReport",
    "iam:GetAccountAuthorizationDetails",
    "iam:GetAccessKeyLastUsed",
    "iam:GetCredentialReport",
    "iam:GetGroupPolicy",
    "iam:GetPolicy",
    "iam:GetPolicyVersion",
    "iam:GetRolePolicy",
    "iam:GetUser",
    "iam:GetUserPolicy",
    "iam:GetAccountPasswordPolicy",
    "iam:GetAccountSummary",
    "iam:ListAttachedGroupPolicies",
    "iam:ListAttachedUserPolicies",
    "iam:ListEntitiesForPolicy",
    "iam:ListGroupsForUser",
    "iam:ListGroupPolicies",
    "iam:ListGroups",
    "iam:ListOpenIdConnectProviders",
    "iam:ListPolicies",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "iam:ListSamlProviders",
    "iam:ListUserPolicies",
    "iam:ListUsers",
    "iam:ListVirtualMFADevices",
    "iam:ListPolicyVersions",
    "iam:ListAccessKeys",
    "iam:ListAttachedRolePolicies",
    "iam:ListMfaDeviceTags",
    "iam:ListMfaDevices",
    "kafka:ListClusters",
    "kafka:ListKafkaVersions",
```

```
    "kinesis:ListStreams",
    "kms:DescribeKey",
    "kms:GetKeyPolicy",
    "kms:GetKeyRotationStatus",
    "kms:ListGrants",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "lambda:ListFunctions",
    "license-manager:ListAssociationsForLicenseConfiguration",
    "license-manager:ListLicenseConfigurations",
    "license-manager:ListUsageForLicenseConfiguration",
    "logs:DescribeDestinations",
    "logs:DescribeExportTasks",
    "logs:DescribeLogGroups",
    "logs:DescribeMetricFilters",
    "logs:DescribeResourcePolicies",
    "logs:FilterLogEvents",
    "logs:GetDataProtectionPolicy",
    "es:DescribeDomains",
    "es:DescribeDomain",
    "es:DescribeDomainConfig",
    "es:ListDomainNames",
    "organizations:DescribeOrganization",
    "organizations:DescribePolicy",
    "rds:DescribeCertificates",
    "rds:DescribeDBClusterEndpoints",
    "rds:DescribeDBClusterParameterGroups",
    "rds:DescribeDBInstances",
    "rds:DescribeDBSecurityGroups",
    "rds:DescribeDBClusters",
    "rds:DescribeDBInstanceAutomatedBackups",
    "redshift:DescribeClusters",
    "redshift:DescribeClusterSnapshots",
    "redshift:DescribeLoggingStatus",
    "route53:GetQueryLoggingConfig",
    "sagemaker:DescribeAlgorithm",
    "sagemaker:DescribeFlowDefinition",
    "sagemaker:DescribeHumanTaskUi",
    "sagemaker:DescribeModelBiasJobDefinition",
    "sagemaker:DescribeModelCard",
    "sagemaker:DescribeModelQualityJobDefinition",
    "sagemaker:DescribeDomain",
    "sagemaker:DescribeEndpoint",
    "sagemaker:DescribeEndpointConfig",
```

```
    "sagemaker:DescribeLabelingJob",
    "sagemaker:DescribeModel",
    "sagemaker:DescribeTrainingJob",
    "sagemaker:DescribeUserProfile",
    "sagemaker:ListAlgorithms",
    "sagemaker:ListDomains",
    "sagemaker:ListEndpoints",
    "sagemaker:ListEndpointConfigs",
    "sagemaker:ListFlowDefinitions",
    "sagemaker:ListHumanTaskUis",
    "sagemaker:ListLabelingJobs",
    "sagemaker:ListModels",
    "sagemaker:ListModelBiasJobDefinitions",
    "sagemaker:ListModelCards",
    "sagemaker:ListModelQualityJobDefinitions",
    "sagemaker:ListMonitoringAlerts",
    "sagemaker:ListMonitoringSchedules",
    "sagemaker:ListTrainingJobs",
    "sagemaker:ListUserProfiles",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketVersioning",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:ListAllMyBuckets",
    "secretsmanager:DescribeSecret",
    "secretsmanager:ListSecrets",
    "securityhub:DescribeStandards",
    "sns:ListTagsForResource",
    "sns:ListTopics",
    "sqs:ListQueues",
    "waf-regional:GetRule",
    "waf-regional:GetWebAcl",
    "waf:GetRule",
    "waf:GetRuleGroup",
    "waf:ListActivatedRulesInRuleGroup",
    "waf:ListWebAcls",
    "wafv2:ListWebAcls",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:ListRuleGroups",
    "waf-regional:ListSubscribedRuleGroups",
    "waf-regional:ListWebACLs",
    "waf-regional:ListRules",
    "waf:ListRuleGroups",
    "waf:ListRules"
```

```
    ],
    "Resource": "*",
    "Sid": "APIsAccess"
   },
   {
    "Sid": "S3Access",
    "Effect": "Allow",
    "Action": [
     "s3:GetBucketAcl",
     "s3:GetBucketLogging",
     "s3:GetBucketOwnershipControls",
     "s3:GetBucketPolicy",
     "s3:GetBucketTagging"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": [
       "${aws:PrincipalAccount}"
      ]
     }
    }
   },
   {
    "Sid": "APIGatewayAccess",
    "Effect": "Allow",
    "Action": [
     "apigateway:GET"
    ],
    "Resource": [
     "arn:aws:apigateway:*::/restapis",
     "arn:aws:apigateway:*::/restapis/*/stages/*",
     "arn:aws:apigateway:*::/restapis/*/stages"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": [
       "${aws:PrincipalAccount}"
      ]
     }
    }
   },
   {
    "Sid": "CreateEventsAccess",
```

```
    "Effect": "Allow",
    "Action": [
     "events:PutRule"
    ],
    "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
    "Condition": {
     "StringEquals": {
      "events:detail-type": "Security Hub Findings - Imported"
     },
     "Null": {
      "events:source": "false"
     },
     "ForAllValues:StringEquals": {
      "events:source": [
       "aws.securityhub"
      ]
     }
    }
   },
   {
    "Sid": "EventsAccess",
    "Effect": "Allow",
    "Action": [
     "events:DeleteRule",
     "events:DescribeRule",
     "events:EnableRule",
     "events:DisableRule",
     "events:ListTargetsByRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
   }
  ]
}
```

AWS Audit Manager mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AWS Audit Manager depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Historique du AWS Audit Manager document.

Modification	Description	Date
AWSAuditManagerServiceRolePolicy – Mise à jour d'une stratégie existante	Nous avons ajouté les autorisations suivantes à`AWSAuditManagerServiceRolePolicy` . AWS Audit Manager peut désormais effectuer les actions suivantes pour collecter des preuves automatisées sur les ressources de votre Compte AWS. • `sagemaker:DescribeAlgorithm` • `sagemaker:DescribeDomain` • `sagemaker:DescribeEndpoint` • `sagemaker:DescribeFlowDefinition` • `sagemaker:DescribeHumanTaskUi` • `sagemaker:DescribeLabelingJob` • `sagemaker:DescribeModel` • `sagemaker:DescribeModelBiasJobDefinition` • `sagemaker:DescribeModelCard` • `sagemaker:DescribeModelQualityJobDefinition` • `sagemaker:DescribeTrainingJob` • `sagemaker:DescribeUserProfile` • `sagemaker:ListAlgorithms` • `sagemaker:ListDomains` • `sagemaker:ListEndpoints` • `sagemaker:ListFlowDefinitions` • `sagemaker:ListHumanTaskUis` • `sagemaker:ListLabelingJobs` • `sagemaker:ListModels`	10/06/2024

Modification	Description	Date
	• sagemaker:ListModelBiasJobDefinitions • sagemaker:ListModelCards • sagemaker:ListModelQualityJobDefinitions • sagemaker:ListMonitoringAlerts • sagemaker:ListMonitoringSchedules • sagemaker:ListTrainingJobs • sagemaker:ListUserProfiles	

Modification	Description	Date
AWSAuditManagerServiceRolePolicy – Mise à jour d'une politique existante	Nous avons ajouté les autorisations suivantes à`AWSAuditManagerServiceRolePolicy` . AWS Audit Manager peut désormais effectuer les actions suivantes pour collecter des preuves automatisées sur les ressources de votre Compte AWS. • `iam:ListAttachedGroupPolicies` • `iam:ListAttachedUserPolicies` • `iam:ListGroupsForUser` • `es:ListDomainNames` Nous avons également ajouté une nouvelle ressource dans la `APIGatewayAccess` section de la politique (`arn:aws:apigateway:*::/restapis`). La politique accorde désormais l'autorisation spécifiée (dans ce cas, l'`apigateway:GET` action) non seulement sur les étapes et les ressources d'étape des API REST d'API Gateway, mais également sur les API REST elles-mêmes. Ce changement élargit effectivement le champ d'application de la politique pour inclure la possibilité de récupérer des informations sur les API REST API Gateway elles-mêmes, en plus des étapes et des ressources d'étape associées à ces API.	17/05/2024

Modification	Description	Date
AWSAuditManagerAdministratorAccess – Mise à jour d'une politique existante	Nous avons ajouté à `AWSAuditManagerAdministratorAccess` les autorisations suivantes : • `controlcatalog:ListCommonControls` • `controlcatalog:ListDomains` • `controlcatalog:ListObjectives` Cette mise à jour vous permet de visualiser les domaines de contrôle, les objectifs de contrôle et les contrôles courants fournis par AWS Control Catalog. Ces autorisations sont requises si vous souhaitez utiliser la fonctionnalité de contrôle commun dans AWS Audit Manager.	15/05/2024

Modification	Description	Date
AWSAuditManagerServiceRolePolicy – Mise à jour d'une politique existante	Nous avons ajouté les autorisations suivantes àAWSAuditManagerServiceRolePolicy . AWS Audit Manager peut désormais effectuer les actions suivantes pour collecter des preuves automatisées sur les ressources de votre Compte AWS. • apigateway:GET • autoscaling:DescribeAutoScalingGroups • backup:ListBackupPlans • cloudfront:GetDistribution • cloudfront:GetDistributionConfig • cloudfront:ListDistributions • cloudtrail:GetTrail • cloudtrail:ListTrails • dynamodb:DescribeContinuousBackups • dynamodb:DescribeBackup • dynamodb:DescribeTableReplicaAutoScaling • ec2:DescribeInstanceCreditSpecifications • ec2:DescribeInstanceAttribute • ec2:DescribeSecurityGroupRules • ec2:DescribeVpcEndpointConnections • ec2:DescribeVpcEndpointServiceConfigurations • ec2:GetLaunchTemplateData	15/05/2024

Modification	Description	Date
	• es:DescribeDomains • es:DescribeDomain • es:DescribeDomainConfig • iam:GetAccessKeyLastUsed • iam:GetGroupPolicy • iam:GetPolicy • iam:GetPolicyVersion • iam:GetRolePolicy • iam:GetUser • iam:GetUserPolicy • iam:ListAccessKeys • iam:ListAttachedRolePolicies • iam:ListMfaDeviceTags • iam:ListMfaDevices • iam:ListPolicyVersions • logs:GetDataProtectionPolicy • rds:DescribeDBInstanceAutomatedBackups • rds:DescribeDBClusterEndpoints • rds:DescribeDBClusterParameterGroups • redshift:DescribeClusterSnapshots • redshift:DescribeLoggingStatus • s3:GetBucketAcl • s3:GetBucketLogging • s3:GetBucketOwnershipControls • s3:GetBucketTagging • sagemaker:DescribeEndpointConfig	

Modification	Description	Date
	• `sagemaker:ListEndpointConfigs` • `secretsmanager:DescribeSecret` • `secretsmanager:ListSecrets` • `sns:ListTagsForResource` • `waf-regional:GetRule` • `waf-regional:GetWebAcl` • `waf-regional:ListRules` • `waf:GetRule` • `waf:GetRuleGroup` • `waf:ListRuleGroups` • `waf:ListRules` • `waf:ListWebAcls` • `wafv2:ListWebAcls`	
AWSAuditManagerServiceRolePolicy – Mise à jour d'une politique existante	Le rôle lié au service permet désormais d' AWS Audit Manager effectuer l'`s3:GetBucketPolicy` action. Cette action d'API est nécessaire pour prendre en charge le framework des bonnes pratiques en matière d'IA générative AWS v1. Cela permet à Audit Manager de collecter des preuves automatisées concernant les restrictions de politiques relatives aux jeux de données d'entraînement de vos modèles d'IA générative. L'`GetBucketPolicy` action fonctionne dans le cadre de l' Compte AWS endroit où elle service-linked-role est disponible. Elle ne peut pas accéder aux politiques de compartiments intercompte.	12/06/2023

Modification	Description	Date
AWSAuditManagerServiceRolePolicy – Mise à jour d'une politique existante	Nous avons ajouté les autorisations suivantes àAWSAuditManagerServiceRolePolicy . AWS Audit Manager peut désormais effectuer les actions suivantes pour collecter des preuves automatisées sur les ressources de votre Compte AWS. • acm:GetAccountConfiguration • acm:ListCertificates • backup:ListRecoveryPointsByResource • bedrock:GetCustomModel • bedrock:GetFoundationModel • bedrock:GetModelCustomizationJob • bedrock:GetModelInvocationLoggingConfiguration • bedrock:ListCustomModels • bedrock:ListFoundationModels • bedrock:ListModelCustomizationJobs • cloudtrail:LookupEvents • cloudwatch:DescribeAlarmsForMetric • cloudwatch:GetMetricStatistics • cloudwatch:ListMetrics • directconnect:DescribeDirectConnectGateways • directconnect:DescribeVirtualGateways • dynamodb:ListBackups	06/11/2023

Modification	Description	Date
	• dynamodb:ListGlobalTables • ec2:DescribeAddresses • ec2:DescribeCustomerGateways • ec2:DescribeEgressOnlyInternetGateways • ec2:DescribeInternetGateways • ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations • ec2:DescribeLocalGateways • ec2:DescribeLocalGatewayVirtualInterfaces • ec2:DescribeNatGateways • ec2:DescribeTransitGateways • ec2:DescribeVpcPeeringConnections • ec2:DescribeVpnConnections • ec2:DescribeVpnGateways • ec2:GetEbsDefaultKmsKeyId • ec2:GetEbsEncryptionByDefault • ecs:DescribeClusters • eks:DescribeAddonVersions • elasticache:DescribeCacheClusters • elasticache:DescribeServiceUpdates • elasticfilesystem:DescribeAccessPoints • elasticloadbalancing:DescribeLoadBalancers	

Modification	Description	Date
	• elasticloadbalancing:DescribeSslPolicies • elasticloadbalancing:DescribeTargetGroups • elasticmapreduce:ListClusters • elasticmapreduce:ListSecurityConfigurations • events:ListConnections • events:ListEventBuses • events:ListEventSources • events:ListRules • firehose:ListDeliveryStreams • fsx:DescribeFileSystems • iam:GetAccountPasswordPolicy • iam:GetCredentialReport • iam:ListOpenIdConnectProviders • iam:ListSamlProviders • iam:ListVirtualMFADevices • kafka:ListClusters • kafka:ListKafkaVersions • kinesis:ListStreams • lambda:ListFunctions • logs:DescribeDestinations • logs:DescribeExportTasks • logs:DescribeLogGroups • logs:DescribeMetricFilters • logs:DescribeResourcePolicies • logs:FilterLogEvents • rds:DescribeCertificates	

Modification	Description	Date
	• rds:DescribeDbClusterEndpoints • rds:DescribeDbClusterParameterGroups • rds:DescribeDbClusters • rds:DescribeDbSecurityGroups • redshift:DescribeClusters • s3:GetBucketPublicAccessBlock • s3:GetBucketVersioning • sns:ListTopics • sqs:ListQueues • waf-regional:GetLoggingConfiguration • waf-regional:ListRuleGroups • waf-regional:ListSubscribedRuleGroups • waf-regional:ListWebACLs	
AWSAuditManagerServiceRolePolicy – Mise à jour d'une politique existante	Nous avons ajouté à AWSAuditManagerServiceRolePolicy les autorisations suivantes : • dynamodb:DescribeTable • dynamodb:ListTables • ec2:DescribeVolumes • kms:GetKeyPolicy • kms:GetKeyRotationStatus • kms:ListKeyPolicies • rds:DescribeDBInstances • redshift:DescribeClusters • s3:GetEncryptionConfiguration • s3:ListAllMyBuckets	07/07/2022

Modification	Description	Date
AWSAuditManagerServiceRolePolicy – Mise à jour d'une politique existante	Le rôle lié au service permet désormais d' AWS Audit Manager effectuer l'`organizations:DescribeOrganization` action. Nous avons également réduit la ressource `CreateEventsAccess` d'un caractère générique (`*`) à un type de ressource spécifique (`arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver`). Enfin, nous avons ajouté un opérateur de condition `Null` pour la clé de condition `events:source` afin de vérifier qu'une valeur source existe et que sa valeur n'est pas nulle.	20/05/2022
AWSAuditManagerAdministratorAccess – Mise à jour d'une politique existante	Nous avons mis à jour la politique relative aux conditions de clés pour `events:source` pour indiquer qu'il s'agit d'une clé à valeurs multiples .	29/04/2022
AWSAuditManagerServiceRolePolicy – Mise à jour d'une politique existante	Nous avons mis à jour la politique relative aux conditions de clés pour `events:source` pour indiquer qu'il s'agit d'une clé à valeurs multiples .	16/03/2022
AWS Audit Manager a commencé à suivre les modifications	AWS Audit Manager a commencé à suivre les modifications apportées AWS à ses politiques gérées.	06/05/2021

Résolution des problèmes AWS Audit Manager d'identité et d'accès

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Audit Manager et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AWS Audit Manager
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AWS Audit Manager ressources

Je ne suis pas autorisé à effectuer une action dans AWS Audit Manager

L'`AccessDeniedException`erreur apparaît lorsqu'un utilisateur n'est pas autorisé à utiliser AWS Audit Manager les opérations de l'API Audit Manager.

Dans ce cas, votre administrateur doit mettre à jour la politique pour autoriser votre accès.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter l'action `iam:PassRole`, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à Audit Manager.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Audit Manager. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AWS Audit Manager ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Audit Manager prend en charge ces fonctionnalités, consultez Comment AWS Audit Manager fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Utilisation de rôles liés à un service pour AWS Audit Manager

AWS Audit Manager utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM lié directement à Audit Manager. Les rôles liés à un service sont prédéfinis par Audit Manager et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration AWS Audit Manager car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Audit Manager définit les autorisations de ses rôles liés à un service ; sauf définition contraire, seul Audit Manager peut endosser ses rôles. Les autorisations

définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez AWS Services qui fonctionnent avec IAM et recherchez les services avec un Oui dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour AWS Audit Manager

Audit Manager utilise le rôle lié au service nommé**`AWSServiceRoleForAuditManager`**, qui permet d'accéder aux services AWS et aux ressources utilisés ou gérés par. AWS Audit Manager

Le rôle lié à un service `AWSServiceRoleForAuditManager` fait confiance au service `auditmanager.amazonaws.com` pour endosser le rôle.

La politique d'autorisation des rôles permet à Audit Manager de collecter des preuves automatisées concernant votre AWS utilisation. `AWSAuditManagerServiceRolePolicy` Plus précisément, il peut effectuer les actions suivantes en votre nom.

- L'Audit Manager peut l'utiliser AWS Security Hub pour collecter des preuves de contrôle de conformité. Dans ce cas, Audit Manager utilise l'autorisation suivante pour signaler les résultats des contrôles de sécurité directement depuis AWS Security Hub. Il joint ensuite les résultats à vos contrôles d'évaluation pertinents à titre d'éléments probants.
  - `securityhub:DescribeStandards`

  > **Note**
  >
  > Pour plus d'informations sur les contrôles Security Hub spécifiques qu'Audit Manager peut décrire, consultez la section AWS Security Hub Contrôles pris en charge par AWS Audit Manager.

- L'Audit Manager peut l'utiliser AWS Config pour collecter des preuves de contrôle de conformité. Dans ce cas, Audit Manager utilise les autorisations suivantes pour communiquer les résultats des évaluations des AWS Config règles directement à partir de AWS Config. Il joint ensuite les résultats à vos contrôles d'évaluation pertinents à titre d'éléments probants.
  - `config:DescribeConfigRules`
  - `config:DescribeDeliveryChannels`

- `config:ListDiscoveredResources`

> **Note**
>
> Pour plus d'informations sur les AWS Config règles spécifiques qu'Audit Manager peut décrire, consultez la section AWS Config Règles prises en charge par AWS Audit Manager.

- Audit Manager peut être utilisé AWS CloudTrail pour collecter des preuves de l'activité des utilisateurs. Dans ce cas, Audit Manager utilise les autorisations suivantes pour capturer l'activité des utilisateurs à partir CloudTrail des journaux. Il joint ensuite l'activité à vos contrôles d'évaluation pertinents à titre d'élément probant.
  - `cloudtrail:DescribeTrails`
  - `cloudtrail:LookupEvents`

> **Note**
>
> Pour plus d'informations sur les CloudTrail événements spécifiques qu'Audit Manager peut décrire, consultez les noms AWS CloudTrail d'événements pris en charge par AWS Audit Manager.

- Audit Manager peut utiliser des appels AWS d'API pour collecter des preuves de configuration des ressources. Dans ce cas, Audit Manager utilise les autorisations suivantes pour appeler des API en lecture seule décrivant vos configurations de ressources pour les Services AWS suivants. Il joint ensuite les réponses de l'API à vos contrôles d'évaluation pertinents à titre d'éléments probants.
  - `acm:GetAccountConfiguration`
  - `acm:ListCertificates`
  - `apigateway:GET`
  - `autoscaling:DescribeAutoScalingGroups`
  - `backup:ListBackupPlans`
  - `backup:ListRecoveryPointsByResource`
  - `bedrock:GetCustomModel`
  - `bedrock:GetFoundationModel`
  - `bedrock:GetModelCustomizationJob`
  - `bedrock:GetModelInvocationLoggingConfiguration`

- bedrock:ListCustomModels
- bedrock:ListFoundationModels
- bedrock:ListModelCustomizationJobs
- cloudfront:GetDistribution
- cloudfront:GetDistributionConfig
- cloudfront:ListDistributions
- cloudtrail:DescribeTrails
- cloudtrail:GetTrail
- cloudtrail:ListTrails
- cloudtrail:LookupEvents
- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeBackup
- dynamodb:DescribeContinuousBackups
- dynamodb:DescribeTable
- dynamodb:DescribeTableReplicaAutoScaling
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways

- ec2:DescribeFlowLogs
- ec2:DescribeInstanceCreditSpecifications
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSecurityGroupRules
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcEndpointConnections
- ec2:DescribeVpcEndpointServiceConfigurations
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ec2:GetLaunchTemplateData
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates

- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- es:DescribeDomains
- es:DescribeDomain
- es:DescribeDomainConfig
- es:ListDomainNames
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccessKeyLastUsed
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy

- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:GetGroupPolicy
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:GetRolePolicy
- iam:GetUser
- iam:GetUserPolicy
- iam:ListAccessKeys
- iam:ListAttachedGroupPolicies
- iam:ListAttachedRolePolicies
- iam:ListAttachedUserPolicies
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListGroupsForUser
- iam:ListMfaDeviceTags
- iam:ListMfaDevices
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListPolicyVersions
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams

- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- logs:GetDataProtectionPolicy
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDBClusterEndpoints
- rds:DescribeDBClusterParameterGroups
- rds:DescribeDBClusters
- rds:DescribeDBInstances
- rds:DescribeDBInstanceAutomatedBackups
- rds:DescribeDBSecurityGroups
- redshift:DescribeClusters
- redshift:DescribeClusterSnapshots
- redshift:DescribeLoggingStatus
- route53:GetQueryLoggingConfig

- s3:GetBucketAcl
- s3:GetBucketLogging
- s3:GetBucketOwnershipControls
- s3:GetBucketPolicy
  - Cette action d'API fonctionne dans le cadre de l' Compte AWS endroit où elle service-linked-role est disponible. Elle ne peut pas accéder aux politiques de compartiments intercompte.
- s3:GetBucketPublicAccessBlock
- s3:GetBucketTagging
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- sagemaker:DescribeAlgorithm
- sagemaker:DescribeDomain
- sagemaker:DescribeEndpoint
- sagemaker:DescribeEndpointConfig
- sagemaker:DescribeFlowDefinition
- sagemaker:DescribeHumanTaskUi
- sagemaker:DescribeLabelingJob
- sagemaker:DescribeModel
- sagemaker:DescribeModelBiasJobDefinition
- sagemaker:DescribeModelCard
- sagemaker:DescribeModelQualityJobDefinition
- sagemaker:DescribeTrainingJob
- sagemaker:DescribeUserProfile
- sagemaker:ListAlgorithms
- sagemaker:ListDomains
- sagemaker:ListEndpointConfigs
- sagemaker:ListEndpoints

- sagemaker:ListFlowDefinitions

- sagemaker:ListHumanTaskUis
- sagemaker:ListLabelingJobs
- sagemaker:ListModels
- sagemaker:ListModelBiasJobDefinitions
- sagemaker:ListModelCards
- sagemaker:ListModelQualityJobDefinitions
- sagemaker:ListMonitoringAlerts
- sagemaker:ListMonitoringSchedules
- sagemaker:ListTrainingJobs
- sagemaker:ListUserProfiles
- securityhub:DescribeStandards
- secretsmanager:DescribeSecret
- secretsmanager:ListSecrets
- sns:ListTagsForResource
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:GetRule
- waf-regional:GetWebAcl
- waf-regional:ListRuleGroups
- waf-regional:ListRules
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:GetRule
- waf:GetRuleGroup
- waf:ListActivatedRulesInRuleGroup
- waf:ListRuleGroups
- waf:ListRules
- waf:ListWebAcls
- wafv2:ListWebAcls

> **Note**
>
> Pour plus d'informations sur les appels d'API spécifiques qu'Audit Manager peut décrire, veuillez consulter Appels d'API pris en charge pour les sources de données de contrôle personnalisées.

Pour consulter les détails complets des autorisations du rôle lié au service`AWSServiceRoleForAuditManager`, consultez le Guide AWSAuditManagerServiceRolePolicyde référence des politiques AWS gérées.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création du rôle lié à AWS Audit Manager un service

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous l'activez AWS Audit Manager, le service crée automatiquement le rôle lié au service pour vous. Vous pouvez activer Audit Manager depuis la page d'accueil du AWS Management Console, ou via l'API ou AWS CLI. Pour plus d'informations, consultez la section Activant AWS Audit Manager de ce guide.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte.

Modification du rôle lié à AWS Audit Manager un service

AWS Audit Manager ne vous permet pas de modifier le rôle `AWSServiceRoleForAuditManager` lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour en savoir plus, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Pour permettre à une entité IAM de modifier la description du rôle lié à un service **`AWSServiceRoleForAuditManager`**

Ajoutez l'instruction suivante à la stratégie d'autorisation de l'entité IAM qui doit modifier la description d'un rôle lié à un service.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "auditmanager.amazonaws.com"}}
}
```

Supprimer le rôle lié à AWS Audit Manager un service

Si vous n'utilisez plus Audit Manager, nous vous recommandons de supprimer le rôle lié à un service `AWSServiceRoleForAuditManager`. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer votre rôle lié à un service avant de pouvoir le supprimer.

Nettoyage du rôle lié au service

Avant de pouvoir utiliser IAM pour supprimer un rôle lié à un service Audit Manager, vous devez d'abord vérifier qu'aucune session n'est active pour le rôle et supprimer toutes les ressources utilisées par le rôle. Pour ce faire, assurez-vous que l'Audit Manager est complètement désenregistré. Régions AWS Après le désenregistrement, Audit Manager n'utilise plus le rôle lié au service.

Pour obtenir des instructions sur le désenregistrement d'Audit Manager, veuillez consulter les ressources suivantes :

- Désactivation AWS Audit Manager dans ce guide
- DeregisterAccount dans la Référence d'API AWS Audit Manager
- désenregistrer un compte dans la référence pour AWS CLI AWS Audit Manager

Pour savoir comment supprimer manuellement les ressources d'Audit Manager, consultez la section Suppression des données d'Audit Manager dans ce guide.

Suppression du rôle lié à un service

Vous pouvez supprimer le rôle lié à un service à l'aide de la console IAM, de l' AWS Command Line Interface (AWS CLI) ou de l'API IAM.

IAM console

Suivez les étapes suivantes pour supprimer le rôle lié à un service dans la console IAM.

Pour supprimer un rôle lié à un service (console)

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation de la console IAM, sélectionnez Roles (Rôles). Sélectionnez la case à cocher en regard de `AWSServiceRoleForAuditManager`, et non le nom ou la ligne.
3. Sous Actions de rôle en haut de la page, sélectionnez Supprimer.
4. Dans la boîte de dialogue de confirmation, vérifiez les dernières informations consultées, indiquant le moment où chacun des rôles sélectionnés a accédé en dernier à un Service AWS. Cela vous permet de confirmer si le rôle est actif actuellement. Si vous souhaitez continuer, saisissez **`AWSServiceRoleForAuditManager`** dans le champ à renseigner, et choisissez Supprimer pour lancer la suppression du rôle lié au service.
5. Consultez les notifications de la console IAM pour surveiller la progression de la suppression du rôle lié à un service. Dans la mesure où la suppression du rôle lié à un service IAM est asynchrone, une fois que vous soumettez le rôle afin qu'il soit supprimé, la suppression peut réussir ou échouer. Si la tâche réussit, le rôle est supprimé de la liste et une notification de succès s'affiche en haut de la page.

AWS CLI

Vous pouvez utiliser les commandes IAM depuis le AWS CLI pour supprimer un rôle lié à un service.

Pour supprimer un rôle lié à un service (AWS CLI)

1. Saisissez la commande suivante pour répertorier le rôle dans votre compte :

```
aws iam get-role --role-name AWSServiceRoleForAuditManager
```

2. Un rôle lié à un service ne pouvant pas être supprimé s'il est utilisé ou si des ressources lui sont associées, vous devez envoyer une demande de suppression. Cette demande peut être refusée si ces conditions ne sont pas remplies. Vous devez capturer le `deletion-task-id` de la réponse afin de vérifier l'état de la tâche de suppression.

Saisissez la commande suivante pour envoyer une demande de suppression d'un rôle lié à un service :

```
aws iam delete-service-linked-role --role-name AWSServiceRoleForAuditManager
```

3. Saisissez la commande suivante pour vérifier l'état de la tâche de suppression :

```
aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```

L'état de la tâche de suppression peut être `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED` ou `FAILED`. Si la suppression échoue, l'appel renvoie le motif de l'échec, afin que vous puissiez apporter une solution.

IAM API

Vous pouvez utiliser l'API IAM pour supprimer un rôle lié à un service.

Pour supprimer un rôle lié à un service (API)

1. Appelez GetRolepour répertorier le rôle dans votre compte. Dans la demande, spécifiez `AWSServiceRoleForAuditManager` en tant que `RoleName`.
2. Un rôle lié à un service ne pouvant pas être supprimé s'il est utilisé ou si des ressources lui sont associées, vous devez envoyer une demande de suppression. Cette demande peut être refusée si ces conditions ne sont pas remplies. Vous devez capturer le `DeletionTaskId` de la réponse afin de vérifier l'état de la tâche de suppression.

   Pour soumettre une demande de suppression pour un rôle lié à un service, appelez. DeleteServiceLinkedRole Dans la demande, spécifiez `AWSServiceRoleForAuditManager` en tant que `RoleName`.
3. Pour vérifier l'état de la suppression, appelez GetServiceLinkedRoleDeletionStatus. Dans la demande, spécifiez le `DeletionTaskId`.

   L'état de la tâche de suppression peut être `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED` ou `FAILED`. Si la suppression échoue, l'appel renvoie le motif de l'échec, afin que vous puissiez apporter une solution.

Conseils pour supprimer le rôle lié au service Audit Manager

Le processus de suppression du rôle lié au service Audit Manager peut échouer si Audit Manager utilise le rôle ou dispose de ressources associées. Cela peut se produire dans les scénarios suivants :

1. Votre compte est toujours enregistré auprès d'Audit Manager dans un ou plusieurs comptes Régions AWS.
2. Votre compte fait partie d'une AWS organisation, et le compte de gestion ou le compte d'administrateur délégué est toujours intégré à Audit Manager.

Pour résoudre un problème de suppression ayant échoué, commencez par vérifier si vous Compte AWS faites partie d'une organisation. Vous pouvez le faire en appelant l'opération DescribeOrganizationAPI ou en accédant à la AWS Organizations console.

Si vous Compte AWS faites partie d'une organisation

1. Utilisez votre compte de gestion pour supprimer votre administrateur délégué dans Audit Manager partout Régions AWS où vous en avez ajouté un.
2. Utilisez votre compte de gestion pour désenregistrer Audit Manager dans tous les Régions AWS endroits où vous avez utilisé le service.
3. Réessayez de supprimer le rôle lié à un service en suivant les étapes de la procédure précédente.

Si vous Compte AWS ne faites pas partie d'une organisation

1. Assurez-vous d'avoir désenregistré Audit Manager dans tous les Régions AWS endroits où vous avez utilisé le service.
2. Réessayez de supprimer le rôle lié à un service en suivant les étapes de la procédure précédente.

Une fois que vous vous êtes désinscrit d'Audit Manager, le service cesse d'utiliser le rôle lié au service. Vous pouvez ensuite supprimer le rôle avec succès.

Régions prises en charge pour les rôles AWS Audit Manager liés à un service

AWS Audit Manager prend en charge l'utilisation de rôles liés au service partout Régions AWS où le service est disponible. Pour plus d'informations, consultez Points de terminaison du service AWS.

Validation de conformité pour AWS Audit Manager

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans plusieurs cadres (notamment le National Institute of Standards and Technology (NIST), le Payment

Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).

- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Comprendre la résilience dans AWS Audit Manager

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant.

Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Sécurité de l'infrastructure dans AWS Audit Manager

En tant que service géré, AWS Audit Manager est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à AWS Audit Manager via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Vous pouvez appeler ces opérations d'API depuis n'importe quel emplacement réseau, mais AWS Audit Manager elles prennent en charge les politiques d'accès basées sur les ressources, qui peuvent inclure des restrictions basées sur l'adresse IP source. Vous pouvez également utiliser des politiques Audit Manager pour contrôler l'accès à partir de points de terminaison Amazon Virtual Private Cloud (Amazon VPC) ou de VPC spécifiques. En fait, cela isole l'accès réseau à une ressource Audit Manager donnée uniquement du VPC spécifique au sein AWS du réseau.

AWS Audit Manager et points de terminaison VPC d'interface ()AWS PrivateLink

Vous pouvez établir une connexion privée entre votre VPC et créer un point de AWS Audit Manager terminaison VPC d'interface. Les points de terminaison d'interface sont alimentés par AWS PrivateLink, une technologie qui vous permet d'accéder en privé aux API Audit Manager sans passerelle Internet, périphérique NAT, connexion VPN ou connexion AWS Direct Connect. Les instances de votre VPC ne requièrent pas d'adresses IP publiques pour communiquer avec les API

Audit Manager. Le trafic entre votre VPC et celui qui AWS Audit Manager ne quitte pas le AWS réseau.

Chaque point de terminaison d'interface est représenté par une ou plusieurs interfaces réseau Elastic dans vos sous-réseaux.

Pour de plus amples informations, consultez Points de terminaison VPC (AWS PrivateLink) dans le Guide de l'utilisateur Amazon VPC.

Considérations relatives aux points de AWS Audit Manager terminaison VPC

Avant de configurer un point de terminaison VPC d'interface pour AWS Audit Manager, assurez-vous de consulter les propriétés et les limites du point de terminaison d'interface dans le guide de l'utilisateur Amazon VPC.

AWS Audit Manager permet d'appeler toutes ses actions d'API depuis votre VPC.

Création d'un point de terminaison de VPC d'interface pour AWS Audit Manager

Vous pouvez créer un point de terminaison VPC pour le AWS Audit Manager service à l'aide de la console Amazon VPC ou du (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Créez un point de terminaison VPC à l' AWS Audit Manager aide du nom de service suivant :

- `com.amazonaws.region.auditmanager`

Si vous activez le DNS privé pour le point de terminaison, vous pouvez envoyer des demandes d'API AWS Audit Manager en utilisant son nom DNS par défaut pour la région, par exemple,`auditmanager.us-east-1.amazonaws.com`.

Pour plus d'informations, consultez Accès à un service via un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Création d'une politique de point de terminaison VPC pour AWS Audit Manager

Vous pouvez attacher une stratégie de point de terminaison à votre point de terminaison d'un VPC qui contrôle l'accès à AWS Audit Manager. La politique spécifie les informations suivantes :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour plus d'informations, consultez Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Exemple : politique de point de terminaison VPC pour les actions AWS Audit Manager

Voici un exemple de politique de point de terminaison pour AWS Audit Manager. Lorsqu'elle est associée à un point de terminaison, cette politique accorde l'accès aux actions Audit Manager répertoriées pour tous les principaux sur toutes les ressources.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "auditmanager:GetAssessment",
            "auditmanager:GetServicesInScope",
            "auditmanager:ListNotifications"
         ],
         "Resource":"*"
      }
   ]
}
```

Connexion et surveillance AWS Audit Manager

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Audit Manager et de vos autres AWS solutions. AWS fournit les outils de surveillance

suivants pour surveiller Audit Manager, signaler un problème et prendre des mesures automatiques le cas échéant :

- AWS CloudTrail capture les appels d'API et les événements associés créés par votre Compte AWS ou au nom de celui-ci et livre les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.
- Amazon EventBridge est un service de bus d'événements sans serveur qui permet de connecter facilement vos applications à des données provenant de diverses sources. EventBridge fournit un flux de données en temps réel à partir de vos propres applications, applications oftware-as-a S-Service (SaaS) et AWS services et achemine ces données vers des cibles telles que Lambda. Cela vous permet de surveiller les événements qui se produisent dans les services et de créer des architectures basées sur les événements. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.

Surveillance AWS Audit Manager avec Amazon EventBridge

Amazon vous EventBridge aide à automatiser Services AWS et à répondre automatiquement aux événements du système tels que les problèmes de disponibilité des applications ou les modifications des ressources.

Vous pouvez utiliser des EventBridge règles pour détecter les événements d'Audit Manager et y réagir. Sur la base des règles que vous créez, EventBridge invoque une ou plusieurs actions cibles lorsqu'un événement correspond aux valeurs que vous spécifiez dans une règle. En fonction du type d'événement, vous pouvez envoyer des notifications, capturer les informations sur l'événement, prendre des mesures correctives, déclencher des événements ou prendre d'autres mesures.

Par exemple, vous pouvez détecter chaque occurrence des événements suivants d'Audit Manager sur votre compte :

- Le responsable d'audit crée, met à jour ou supprime une évaluation
- Le responsable d'audit délègue une série de contrôles à des fins de révision
- Un délégué termine son examen et renvoie la série de contrôles examiné au responsable d'audit.
- Un responsable d'audit met à jour l'état d'un contrôle d'évaluation

Les actions pouvant être déclenchées automatiquement sont les suivantes :

- Utilisez une AWS Lambda fonction pour transmettre une notification à une chaîne Slack.
- Envoyer les données relatives à la vérification à un Amazon Kinesis Data Streams pour prendre en charge la surveillance complète et en temps réel du statut.
- Envoyer une rubrique Amazon Simple Notification Service (Amazon SNS) à votre e-mail.
- Recevez une notification d'une action CloudWatch d'alarme Amazon.

> **Note**
>
> Audit Manager délivre des événements sur une base durable. Cela signifie qu'Audit Manager tentera avec succès de transmettre des événements EventBridge au moins une fois. Dans les cas où les événements ne peuvent pas être transmis en raison d'une interruption de EventBridge service, ils seront réessayés ultérieurement par l'Audit Manager pendant 24 heures au maximum.

EventBridge exemple de format pour Audit Manager

Le code JSON suivant montre un exemple d'événement de création d'évaluation dans Audit Manager. Pour plus d'informations sur l'un des champs de cet événement, voir Référence de structure d'événement.

```
{
    "version": "0",
    "id": "55c5a6f3-6183-3989-49ec-a3c998857644",
    "detail-type": "Assessment Created",
    "source": "aws.auditmanager",
    "account": "111122223333",
    "time": "2023-07-27T00:38:33Z",
    "region": "us-west-2",
    "resources":
        [
            "arn:aws:auditmanager:us-west-2:111122223333:assessment/a1b2c3d4-e5f6-g7h8-
i9j0-k1l2m3n4o5p6"
        ],
    "detail":
    {
        "eventID": "4e939b2f-9429-3141-beec-d640d83ef68e",
        "author": "arn:aws:sts::111122223333:assumed-role/roleName/role-session-name",
        "assessmentTenantId": "111122223333",
```

```
        "assessmentName": "myAssessment",
        "eventTime": 1690418289068,
        "eventName": "CREATE",
        "eventType": "ASSESSMENT",
        "assessmentID": "a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"
    }
}
```

Conditions préalables à la création d'une règle EventBridge

Avant de créer des politiques pour les événements Audit Manager, nous vous recommandons de procéder comme suit :

- Familiarisez-vous avec les événements, les règles et les cibles dans EventBridge. Pour plus d'informations, consultez Qu'est-ce qu'Amazon EventBridge ? dans le guide de EventBridge l'utilisateur Amazon.
- Créez la cible à utiliser dans votre règle d'événement. Par exemple, vous pouvez créer une rubrique Amazon SNS, afin de recevoir un texto ou un e-mail à chaque fois que l'examen d'une série de contrôles est terminé. Pour plus d'informations, consultez la section EventBridge Objectifs.

Création d'une EventBridge règle pour Audit Manager

Suivez ces étapes pour créer une EventBridge règle qui se déclenche lors d'un événement émis par Audit Manager. Les événements sont générés dans la mesure du possible.

Pour créer une EventBridge règle pour Audit Manager

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Dans le volet de navigation, choisissez Règles.
3. Choisissez Créer une règle.
4. Sur la page Définir les informations de la règle, saisissez un nom et une description pour la règle.
5. Conservez les valeurs par défaut pour Bus d'événement et Type de règle, puis choisissez Suivant.
6. Sur la page Créer un modèle d'événement, dans Source d'événement, sélectionnez AWS événements ou événements EventBridge partenaires.
7. Dans Méthode de création, choisissez Modèle personnalisé (éditeur JSON).

8. Dans Modèle d'événement, entrez un modèle d'événement au format JSON et spécifiez les champs que vous souhaitez utiliser pour la correspondance.

   Pour faire correspondre un événement Audit Manager, vous pouvez utiliser le modèle simple suivant :

   ```
   {
     "detail-type": ["Event"]
   }
   ```

   Remplacez *Event* par l'une des valeurs prises en charge suivantes :

   a. Saisissez `Assessment Created` pour recevoir des notifications lorsqu'une évaluation est créée.

   b. Saisissez `Assessment Updated` pour recevoir des notifications lorsqu'une évaluation est mise à jour.

   c. Saisissez `Assessment Deleted` pour recevoir des notifications lorsqu'une évaluation est supprimée.

   d. Saisissez `Assessment ControlSet Delegation Created` pour recevoir des notifications lorsqu'une série de contrôles est déléguée pour examen.

   e. Saisissez `Assessment ControlSet Reviewed` pour recevoir des notifications lorsqu'une série de contrôles d'évaluation est examinée.

   f. Saisissez `Assessment Control Reviewed` pour recevoir des notifications lorsqu'un contrôle d'évaluation est examiné.

   > **Tip**
   >
   > Ajoutez d'autres champs à votre modèle d'événement selon vos besoins. Pour plus d'informations sur les champs disponibles, consultez les modèles EventBridge d'événements Amazon.

9. Choisissez Suivant.

10. Sur la page Sélectionner la ou les cibles, choisissez la cible créée pour cette règle, puis configurez toutes les options supplémentaires requises pour ce type. Par exemple, si vous choisissez Amazon SNS, assurez-vous que votre rubrique SNS est configurée correctement pour être notifié par e-mail ou SMS.

> **Tip**
>
> Les champs affichés varient en fonction du service sélectionné. Pour plus d'informations sur les cibles disponibles, consultez la section Cibles disponibles dans la EventBridge console.

11. Pour de nombreux types de cibles, EventBridge nécessite des autorisations pour envoyer des événements à la cible. Dans ces cas, EventBridge vous pouvez créer le rôle IAM nécessaire à l'exécution de votre règle.

    a. Pour créer un rôle IAM automatiquement, sélectionnez Create a new role for this specific resource.

    b. Pour utiliser un rôle IAM que vous avez créé auparavant, sélectionnez Use existing role (Utiliser un rôle existant).

12. (Facultatif) Sélectionnez Add another target (Ajouter une autre cible) pour ajouter une nouvelle cible pour cette règle.
13. Choisissez Suivant.
14. (Facultatif) Sur la page Configure tags (Configurer des étiquettes), ajoutez des étiquettes, puis choisissez Next (Suivant).
15. Sur la page Vérifier et créer, examinez la configuration de votre règle et assurez-vous qu'elle répond à vos exigences en matière de surveillance d'événements.
16. Choisissez Créer une règle. Votre règle va maintenant surveiller les événements Audit et les envoyer à la cible spécifiée.

Journalisation des appels d' AWS Audit Manager API avec CloudTrail

Audit Manager est intégré à CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS Audit Manager. CloudTrail capture tous les appels d'API pour Audit Manager sous forme d'événements. Les appels capturés incluent les appels de la console Audit Manager et les appels de code vers les opérations d'API d'Audit Manager.

Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Audit Manager. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements.

À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Audit Manager, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur l'Audit Manager dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans Audit Manager, cette activité est enregistrée dans un CloudTrail événement avec d'autres Service AWS événements dans l'historique des événements.

Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre entreprise Compte AWS, y compris des événements pour Audit Manager, créez une trace. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez.

En outre, vous pouvez en configurer d'autres Services AWS pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Vue d'ensemble de la création d'un journal d'activité
- CloudTrail Services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions d'Audit Manager sont enregistrées CloudTrail et documentées dans la référence de l'AWS Audit Manager API. Par exemple, les appels aux opérations `CreateControl`, `DeleteControl`, et `UpdateAssessmentFramework` API génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec les informations d'identification d'utilisateur root.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

Pour plus d'informations, consultez l'élément CloudTrail UserIdentity.

Comprendre les entrées du fichier journal d'Audit Manager

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`CreateAssessment`action.

```
{
      eventVersion:"1.05",
      userIdentity:{
        type:"IAMUser",
        principalId:"principalId",
        arn:"arn:aws:iam::accountId:user/userName",
        accountId:"111122223333",
        accessKeyId:"accessKeyId",
        userName:"userName",
        sessionContext:{
          sessionIssuer:{
          },
          webIdFederationData:{
          },
          attributes:{
            mfaAuthenticated:"false",
            creationDate:"2020-11-19T07:32:06Z"
          }
        }
```

```
      },
      eventTime:"2020-11-19T07:32:36Z",
      eventSource:"auditmanager.amazonaws.com",
      eventName:"CreateAssessment",
      awsRegion:"us-west-2",
      sourceIPAddress:"sourceIPAddress",
      userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
      requestParameters:{
        frameworkId:"frameworkId",
        assessmentReportsDestination:{
          destination:"***",
          destinationType:"S3"
        },
        clientToken:"***",
        scope:{
          awsServices:[
            {
              serviceName:"license-manager"
            }
          ],
          awsAccounts:"***"
        },
        roles:"***",
        name:"***",
        description:"***",
        tags:"***"
      },
      responseElements:{
        assessment:"***"
      },
      requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
      eventID:"a782029a-959e-4549-81df-9f6596775cb0",
      readOnly:false,
      eventType:"AwsApiCall",
      recipientAccountId:"recipientAccountId"
    }
```

Comprendre la configuration et l'analyse des vulnérabilités dans AWS Audit Manager

La configuration et les contrôles informatiques sont une responsabilité partagée entre vous AWS et vous, notre client. Pour plus d'informations, consultez le modèle de responsabilité AWS partagée.

Création de AWS Audit Manager ressources avec AWS CloudFormation

AWS Audit Manager est intégré à AWS CloudFormation un service qui vous aide à modéliser et à configurer vos AWS ressources afin que vous puissiez passer moins de temps à créer et à gérer vos ressources et votre infrastructure. Vous créez un modèle qui décrit toutes les AWS ressources que vous souhaitez (telles que les évaluations), et AWS CloudFormation qui fournit et configure ces ressources pour vous.

Lorsque vous l'utilisez AWS CloudFormation, vous pouvez réutiliser votre modèle pour configurer les ressources de votre Audit Manager de manière cohérente et répétée. Décrivez vos ressources une seule fois, puis fournissez les mêmes ressources à plusieurs reprises dans plusieurs AWS comptes et régions.

Audit Manager et AWS CloudFormation modèles

Pour provisionner et configurer des ressources pour Audit Manager et les services associés, vous devez bien comprendre les AWS CloudFormation modèles. Les modèles sont des fichiers texte formatés en JSON ou YAML. Ces modèles décrivent les ressources que vous souhaitez mettre à disposition dans vos AWS CloudFormation piles. Si vous n'êtes pas familiarisé avec JSON ou YAML, vous pouvez utiliser AWS CloudFormation Designer pour vous aider à démarrer avec les AWS CloudFormation modèles. Pour plus d'informations, consultez Qu'est-ce que AWS CloudFormation Designer ? dans le AWS CloudFormation Guide de l'utilisateur.

Audit Manager prend en charge la création d'évaluations dans AWS CloudFormation. Pour de plus amples informations, y compris des exemples de modèles JSON et YAML pour les évaluations, consultez la rubrique AWS Audit Manager Référence du type de ressource dans le Guide de l'utilisateur AWS CloudFormation .

En savoir plus sur AWS CloudFormation

Pour en savoir plus AWS CloudFormation, consultez les ressources suivantes :

- AWS CloudFormation
- AWS CloudFormation Guide de l'utilisateur
- AWS CloudFormation API Reference

- AWS CloudFormation Guide de l'utilisateur de l'interface de ligne de commande

Utilisation AWS Audit Manager avec un AWS SDK

AWS des kits de développement logiciel (SDK) sont disponibles pour de nombreux langages de programmation populaires. Chaque SDK fournit une API, des exemples de code et de la documentation qui peuvent être utilisés par les développeurs pour créer des applications dans leur langage préféré.

Documentation SDK	cette documentation spécifique à ce service	Exemples de code	
AWS SDK for C++	AWS SDK for C++ Référence d'API pour Audit Manager	AWS SDK for C++ exemples de code	
AWS SDK for Go	AWS SDK for Go Référence d'API pour Audit Manager	AWS SDK for Go exemples de code	
AWS SDK for Java	AWS SDK for Java 2.x Référence d'API pour Audit Manager	AWS SDK for Java exemples de code	
AWS SDK for JavaScript	AWS SDK for JavaScript Référence d'API pour Audit Manager	AWS SDK for JavaScript exemples de code	
AWS SDK for .NET	AWS SDK for .NET Référence d'API pour Audit Manager	AWS SDK for .NET exemples de code	
AWS SDK for PHP	AWS SDK for PHP Référence d'API pour Audit Manager	AWS SDK for PHP exemples de code	
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto) Référence d'API pour Audit Manager	AWS SDK for Python (Boto3) exemples de code	
AWS SDK for Ruby	AWS SDK for Ruby Référence d'API pour Audit Manager	AWS SDK for Ruby exemples de code	

Pour des exemples spécifiques à ce service, consultez les exemples de code pour Audit Manager utilisant AWS des SDK.

> **Note**
>
> Audit Manager est disponible dans les versions 1.19.32 et ultérieures de botocore pour le AWS SDK for Python (Boto3). Avant de commencer à utiliser le SDK, assurez-vous que vous utilisez la version appropriée de botocore.

Désactivation AWS Audit Manager

Vous pouvez désactiver Audit Manager si vous ne souhaitez plus utiliser le service. Lorsque vous désactivez Audit Manager, vous avez également la possibilité de supprimer toutes vos données.

Par défaut, vos données ne sont pas supprimées lorsque vous désactivez Audit Manager. Vos données d'éléments probants sont conservées pendant deux ans à compter de leur création. Vos autres ressources d'Audit Manager (y compris les évaluations, les contrôles personnalisés et les frameworks personnalisés) sont conservées indéfiniment et seront disponibles si vous réactivez Audit Manager ultérieurement. Pour plus d'informations sur la conservation des données, veuillez consulter Protection des données dans ce guide.

Si vous choisissez de supprimer vos données, Audit Manager supprime toutes les données probantes ainsi que toutes les ressources d'Audit Manager que vous avez créées (y compris les évaluations, les contrôles personnalisés et les frameworks personnalisés). Toutes vos données sont supprimées dans les sept jours suivant la désactivation d'Audit Manager.

Rubriques

Procédure

Vous pouvez désactiver Audit Manager à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

⚠ Warning

- Lorsque vous désactivez Audit Manager, votre accès est révoqué et le service ne collecte plus d'éléments probants pour les évaluations existantes. Vous ne pouvez accéder à aucun élément du service à moins de réactiver Audit Manager.
- La suppression de toutes les données est une action permanente. Si vous décidez de réactiver Audit Manager ultérieurement, vos données ne seront pas récupérables.

Audit Manager console

Pour désactiver Audit Manager sur la console Audit Manager

1. Dans l'onglet Paramètres généraux, accédez à la section Désactiver AWS Audit Manager.
2. Choisissez Désactiver.
3. Dans la fenêtre contextuelle, vérifiez votre paramètre actuel de conservation des données.
    a. Pour poursuivre votre sélection actuelle, choisissez Désactiver Audit Manager.
    b. Pour modifier votre sélection actuelle, effectuez les étapes suivantes :
        i. Choisissez Annuler pour revenir à la page des paramètres.
        ii. Pour utiliser le paramètre de conservation des données par défaut, désactivez Supprimer toutes les données. Cette sélection conserve les données probantes pendant deux ans à compter de sa création, et conserve indéfiniment les autres ressources de l'Audit Manager.
        iii. Pour supprimer vos données, activez Supprimer toutes les données.
        iv. Choisissez Désactiver, puis Désactiver Audit Manager pour confirmer votre choix.

AWS CLI

Avant de commencer

Avant de désactiver Audit Manager, vous pouvez exécuter la commande update-settings pour définir votre politique de conservation des données préférée. Par défaut, Audit Manager conserve vos données. Si vous souhaitez demander la suppression de vos données, utilisez le paramètre `--deregistration-policy` dont la valeur `deleteResources` est définie sur `ALL`.

```
aws auditmanager update-settings --deregistration-policy deleteResources=ALL
```

Pour désactiver Audit Manager dans AWS CLI

Lorsque vous êtes prêt à désactiver Audit Manager, exécutez la commande deregister-account.

```
aws auditmanager deregister-account
```

Audit Manager API

Avant de commencer

Avant de désactiver Audit Manager, vous pouvez utiliser l'opération UpdateSettingsd'API pour définir votre politique de conservation des données préférée. Par défaut, Audit Manager conserve vos données. Si vous souhaitez supprimer vos données, vous pouvez utiliser l'DeregistrationPolicyattribut pour demander la suppression de vos données.

Pour désactiver Audit Manager à l'aide de l'API

Lorsque vous êtes prêt à désactiver Audit Manager, appelez l'DeregisterAccountopération.

Pour plus d'informations, choisissez les liens précédents dans le Guide de référence de l'API de l'Audit Manager. Cela inclut des informations sur la façon d'utiliser ces opérations et paramètres dans l'un des SDK spécifiques au langage AWS .

Étapes suivantes

Si vous devez réactiver Audit Manager après l'avoir désactivé, procédez comme suit pour que le service soit à nouveau opérationnel.

Pour réactiver Audit Manager après l'avoir désactivé

Accédez à la page d'accueil du service Audit Manager et suivez les étapes pour configurer Audit Manager en tant que nouvel utilisateur. Pour plus d'informations, consultez Configuration AWS Audit Manager avec les paramètres recommandés.

Tip

- Si vous avez choisi de supprimer vos données lorsque vous avez désactivé Audit Manager, vous devez attendre qu'elles soient supprimées avant de pouvoir réactiver le service. Selon la quantité de données dont vous disposez, cela peut prendre jusqu'à sept jours. Cependant, n'hésitez pas à essayer de réactiver Audit Manager avant cette date. Dans de nombreux cas, les données sont supprimées en une heure seulement.
- Si vous choisissez de ne pas supprimer vos données lorsque vous désactivez Audit Manager, vos évaluations existantes passent à l'état inactif et cessent de collecter des éléments probants. Pour qu'une évaluation préexistante recommence à collecter des éléments probants, modifiez l'évaluation et choisissez Enregistrer sans apporter de modifications.

Ressources supplémentaires

- Pour plus d'informations sur la conservation des données dans Audit Manager, consultez la section Protection des données dans ce guide.

Historique du document pour le guide de AWS Audit Manager l'utilisateur

Le tableau suivant décrit les modifications importantes apportées à chaque version du guide de AWS Audit Manager l'utilisateur à compter du 8 décembre 2020.

Modification	Description	Date
Nouveau framework pris en charge : meilleures pratiques d'IA AWS générative v2	Un nouveau framework prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, consultez le framework de bonnes pratiques d'IA AWS générative v2.	11 juin 2024
Politique AWS gérée mise à jour	AWS Audit Manager a mis à jour le AWSAuditManagerServiceRolePolicy. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Audit Manager.	10 juin 2024
Utilisez des contrôles communs pour simplifier la façon dont vous exécutez les évaluations par rapport aux contrôles de votre entreprise	Lorsque vous créez un contrôle personnalisé, vous pouvez désormais utiliser des contrôles courants comme source de preuves. Chaque contrôle commun correspond à un groupe géré de sources de AWS données pertinentes. Ces groupements prédéfinis rationalisent la collecte de preuves en éliminant le besoin d'identifier les AWS ressources à évaluer pour un contrôle	6 juin 2024

	donné. Pour plus d'informations sur la manière de trouver des contrôles courants et de les utiliser comme sources de preuves, consultez la section Bibliothèque de contrôles.	
Politique AWS gérée mise à jour	AWS Audit Manager a mis à jour le AWSAuditManagerServiceRolePolicy. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Audit Manager.	17 mai 2024
Politique AWS gérée mise à jour	AWS Audit Manager a mis à jour la AWSAuditManagerAdministratorAccesspolitique. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Audit Manager.	15 mai 2024
Politique AWS gérée mise à jour	AWS Audit Manager a mis à jour le AWSAuditManagerServiceRolePolicy. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Audit Manager.	15 mai 2024

Support pour les appels AWS d'API supplémentaires	Vous pouvez désormais utiliser des appels AWS d'API supplémentaires comme sources de données pour vos contrôles personnalisés dans Audit Manager. Pour plus d'informations, veuillez consulter la section Appels d'API pris en charge pour les sources de données de contrôles personnalisés.	15 mai 2024
Nouveau framework pris en charge : PCI DSS V4.0	Un nouveau framework prédéfini est désormais disponible dans AWS Audit Manager. Pour de plus amples informations, consultez la section PCI DSS V4.0.	19 décembre 2023
Support pour les appels AWS d'API supplémentaires	Vous pouvez désormais utiliser des appels AWS d'API supplémentaires comme sources de données pour vos contrôles personnalisés dans Audit Manager. Pour plus d'informations, veuillez consulter la section Appels d'API pris en charge pour les sources de données de contrôles personnalisés.	7 décembre 2023
Politique AWS gérée mise à jour	AWS Audit Manager a mis à jour le AWSAuditManagerServiceRolePolicy. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Audit Manager.	6 décembre 2023

Support pour les résultats de contrôle AWS Security Hub consolidés	Audit Manager prend désormais en charge les contrôles consolidés dans AWS Security Hub. Pour plus d'informations, consultez la section AWS Security Hub Contrôles pris en charge par AWS Audit Manager.	16 novembre 2023
Intégration avec MetricStream	Vous pouvez désormais intégrer des preuves provenant d'Audit Manager dans. MetricStream Pour plus d'informations, veuillez consulter Intégrations avec des produits GRC tiers.	14 novembre 2023
Nouveau cadre pris en charge : meilleures pratiques en matière d'IA AWS générative	Un nouveau framework prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter le AWS cadre des meilleures pratiques en matière d'IA générative v1.	8 novembre 2023
Politique AWS gérée mise à jour	AWS Audit Manager a mis à jour le AWSAuditManagerServiceRolePolicy. Pour plus d'informations, veuillez consulter AWS politiques gérées pour AWS Audit Manager.	6 novembre 2023

Intégration avec Amazon EventBridge	Vous pouvez désormais surveiller les événements qui se produisent dans AWS Audit Manager et utiliser ces événements dans le cadre de votre architecture axée sur les événements. Pour plus d'informations, consultez la section Surveillance AWS Audit Manager avec Amazon EventBridge.	18 août 2023
Support pour les évaluations des risques et les nouvelles options d'éléments probants manuels	Vous pouvez désormais utiliser le flux de travail de création de contrôles personnalisés pour appuyer les évaluations des risques. Un contrôle peut désormais représenter une question d'évaluation des risques, et vous pouvez y répondre en téléchargeant un fichier ou en saisissant du texte comme élément probant manuel. Pour plus d'informations, veuillez consulter Création d'un contrôle personnalisé et Ajouter des éléments probants manuels.	12 juin 2023

Support pour les exportations au format CSV	Vous pouvez désormais exporter les résultats de votre recherche dans l'outil de recherche d'éléments probants au format CSV. Pour plus d'informations, veuillez consulter Exporter vos résultats de recherche.	9 juin 2023
Manuel de sécurité de l'information du Centre australien de cybersécurité (Autralian Cyber Security Centre, ACSC)	Un nouveau framework prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter le manuel de sécurité de l'information du Centre australien de cybersécurité (ACSC).	24 mars 2023
Rapports d'évaluation améliorés	Nous avons amélioré le format et le contenu des rapports d'évaluation d'Audit Manager. Pour plus d'informations sur la navigation et la compréhension des rapports d'évaluation, veuillez consulter Rapports d'évaluation.	23 mars 2023
Support pour les appels d'API paginés	AWS Audit Manager prend désormais en charge les appels d'API paginés en tant que source de données pour la collecte de preuves. Pour plus d'informations, veuillez consulter Appels d'API paginés.	8 mars 2023

Nouveau cadre pris en charge : Règle de sécurité omnibus finale HIPAA 2013	Un nouveau framework prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter la règle de sécurité omnibus finale HIPAA 2013. À des fins de différenciation, le cadre HIPAA existant (anciennement nommé HIPAA dans la bibliothèque de cadres) s'appelle désormais Règle de sécurité HIPAA 2003.	8 mars 2023
Support pour les appels AWS d'API supplémentaires	Vous pouvez désormais utiliser neuf appels d' AWS API supplémentaires comme source de données pour vos contrôles personnalisés dans Audit Manager. Pour plus d'informations, veuillez consulter la section Appels d'API pris en charge pour les sources de données de contrôles personnalisés.	3 mars 2023
Guide mis à jour pour s'aligner sur les bonnes pratiques IAM	Guide mis à jour pour s'aligner sur les bonnes pratiques IAM. Pour plus d'informations, consultez Bonnes pratiques de sécurité dans IAM.	6 janvier 2023

Nouveau paramètre de conservation des données	Vous pouvez désormais spécifier si vous souhaitez supprimer toutes vos données lorsque vous désactivez Audit Manager. Pour plus d'informations, veuillez consulter la section Désactivation AWS Audit Manager et Suppression des données d'Audit Manager.	6 janvier 2023
Support pour l'outil de recherche d'éléments probants	Vous pouvez désormais utiliser l'outil de recherche d'éléments probants pour effectuer des recherches sur vos données d'éléments probants. Pour plus d'informations, veuillez consulter l'outil de recherche d'éléments probants.	18 novembre 2022
Nouveau cadre pris en charge : Essential Eight du Centre australien de cybersécurité (ACSC)	Un nouveau framework prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter Australian Cyber Security Centre (ACSC) Essential Eight.	24 août 2022
Politique AWS gérée mise à jour	AWS Audit Manager a mis à jour le AWSAuditManagerServiceRolePolicy. Pour plus d'informations, veuillez consulter AWS politiques gérées pour AWS Audit Manager.	7 juillet 2022

Politique AWS gérée mise à jour	AWS Audit Manager a mis à jour le AWSAuditManagerServiceRolePolicy. Pour plus d'informations, veuillez consulter AWS politiques gérées pour AWS Audit Manager.	20 mai 2022
Nouveau cadre pris en charge : Profil de contrôle du cloud de taille moyenne du Centre canadien pour la cybersécurité	Un nouveau framework prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter le profil de contrôle du cloud de taille moyenne du Centre canadien pour la cybersécurité.	6 mai 2022
Politique AWS gérée mise à jour	AWS Audit Manager a mis à jour la AWSAuditManagerAdministratorAccesspolitique. Pour plus d'informations, veuillez consulter AWS politiques gérées pour AWS Audit Manager.	29 avril 2022
Support pour des règles AWS Config gérées supplémentaires	Vous pouvez désormais utiliser 91 règles AWS Config gérées supplémentaires comme source de données pour vos contrôles personnalisés dans Audit Manager. Pour plus d'informations, consultez la section Utilisation de règles AWS Config gérées avec AWS Audit Manager.	27 avril 2022

Support pour les règles AWS Config personnalisées	Vous pouvez désormais utiliser AWS Config des règles personnalisées comme source de données pour vos contrôles personnalisés dans Audit Manager. Pour plus d'informations, consultez la section Utilisation de règles AWS Config personnalisées avec AWS Audit Manager.	27 avril 2022
Nouveau cadre pris en charge : ISO/IEC 27001:2013 Annexe A	Un nouveau framework prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter l'annexe A de la norme ISO/IEC 27001:2013.	7 avril 2022
Politique AWS gérée mise à jour	AWS Audit Manager a mis à jour le AWSAuditManagerServiceRolePolicy. Pour plus d'informations, veuillez consulter AWS politiques gérées pour AWS Audit Manager.	16 mars 2022

Nouveaux cadres pris en charge : CIS Benchmark pour CIS Amazon Web Services Foundations Benchmark v1.4	Deux nouveaux frameworks prédéfinis sont désormais disponibles dans AWS Audit Manager : CIS Benchmark pour CIS Amazon Web Services Foundations Benchmark v1.4, Level 1, et CIS Benchmark for CIS Amazon Web Services Foundations Benchmark v1.4, Level 1 et 2. Pour plus d'informations, veuillez consulter CIS Benchmark pour CIS AWS Audit Manager Foundations Benchmark v1.4.0.	2 mars 2022
Nouveau cadre pris en charge : CIS Controls v8 IG1	Un nouveau framework prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter CIS Controls v8 IG1.	2 mars 2022
AWS Audit Manager tableau de bord	Vous pouvez désormais utiliser le tableau de bord d'Audit Manager pour surveiller vos évaluations actives et identifier rapidement les éléments probants non conformes. Pour plus d'informations, veuillez consulter Utiliser le tableau de bord d'Audit Manager.	18 novembre 2021

Partage d'un framework personnalisé	Vous pouvez désormais partager vos frameworks Audit Manager personnalisés avec un autre Compte AWS, ou les répliquer dans un autre Région AWS sous votre propre compte. Pour plus d'informations, veuillez consulter Partage d'un cadre personnalisé.	22 octobre 2021
Nouveaux exemples de AWS Audit Manager contrôles	Vous pouvez désormais consulter des exemples de contrôles et découvrir comment Audit Manager contribue à AWS adapter votre environnement à leurs exigences. Pour plus d'informations, consultez la section Exemples de AWS Audit Manager contrôles.	21 septembre 2021
Nouveau cadre pris en charge : Loi Gramm-Leach-Bliley (GLBA)	Un nouveau framework prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter la Loi Gramm-Leach-Bliley (GLBA).	2 septembre 2021
Nouveau chapitre Résolution des problèmes	Un nouveau chapitre Résolution des problèmes est désormais disponible. Pour plus d'informations, consultez la section Résolution des problèmes dans AWS Audit Manager.	23 août 2021

Nouveau chapitre et tutoriel sur la délégation	Nous avons élargi notre documentation de délégation dans un nouveau chapitre. Pour plus d'informations, voir Délégations dans AWS Audit Manager. Nous avons également ajouté un nouveau didacticiel destiné aux délégués qui examinent un ensemble de contrôles pour la première fois depuis AWS Audit Manager. Pour plus d'informations, veuillez consulter Tutoriel pour les délégués : Révision d'un ensemble de contrôles.	25 juin 2021
Nouveau cadre pris en charge : NIST SP 800-171 Rev. 2	Un nouveau framework prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter NIST SP 800-171 Rev. 2.	17 juin 2021
Rapports d'évaluation améliorés	Nous avons amélioré le format et le contenu des rapports AWS Audit Manager d'évaluation. Pour plus d'informations sur la façon de naviguer dans les nouveaux rapports d'évaluation et de les comprendre, veuillez consulter la section Rapports d'évaluation.	8 juin 2021

Nouvelle page de politiques AWS gérées	AWS Audit Manager a commencé à suivre les modifications apportées à ses politiques gérées. Pour plus d'informations, veuillez consulter Politiques gérées AWS pour AWS Audit Manager.	6 mai 2021
Nouveau cadre pris en charge : Cadre de cybersécurité du NIST version 1.1	Un nouveau framework prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter la version 1.1 du cadre de cybersécurité du NIST.	5 mai 2021
Nouveau framework pris en charge : AWS Well-Architected	Un nouveau framework prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter AWS Bien architecturé.	5 mai 2021
Nouveau framework pris en charge : AWS meilleures pratiques de sécurité de base	Un nouveau framework prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter AWS Bonnes pratiques de sécurité de base.	5 mai 2021

Nouveau cadre pris en charge : GxP UE Annexe 11	Un nouveau framework prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter Annexe 11 de la GxP UE.	28 avril 2021
Nouveau cadre pris en charge : NIST 800-53 (Rév. 5) Faible-modéré-élevé	Un nouveau framework prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter NIST 800-53 (Rév. 5) Faible-modéré-élevé.	25 mars 2021
Nouveaux frameworks pris en charge : CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3	Deux nouveaux frameworks prédéfinis sont désormais disponibles dans AWS Audit Manager : CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0, Level 1, et CIS Benchmark for CIS AWS Audit Manager Foundations Benchmark v1.3.0, Level 1 et 2. Pour plus d'informations, veuillez consulter CIS Benchmark pour CIS AWS Audit Manager Foundations Benchmark v1.3.0.	22 mars 2021
Première version	Publication initiale du guide de l' AWS Audit Manager utilisateur et de la référence d'API.	8 décembre 2020

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.