aws

Guide de l’utilisateur

Amazon Macie

Amazon Macie: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'Amazon Macie ?

Amazon Macie est un service de sécurité des données qui découvre les données sensibles à l'aide du machine learning et de la correspondance de modèles, fournit une visibilité sur les risques liés à la sécurité des données et permet une protection automatisée contre ces risques.

Pour vous aider à gérer le niveau de sécurité du parc de données Amazon Simple Storage Service (Amazon S3) de votre entreprise, Macie vous fournit un inventaire de vos compartiments S3 à usage général et évalue et surveille automatiquement les compartiments pour des raisons de sécurité et de contrôle d'accès. Si Macie détecte un problème potentiel lié à la sécurité ou la confidentialité de vos données, tel qu'un compartiment devenant accessible au public, il génère un résultat que vous devrez examiner et auquel vous pourrez remédier si nécessaire.

Macie automatise également la découverte et le reporting des données sensibles afin de vous permettre de mieux comprendre les données que votre organisation stocke dans Amazon S3. Pour détecter les données sensibles, vous pouvez utiliser des critères et des techniques intégrés fournis par Macie, des critères personnalisés que vous définissez ou une combinaison des deux. Si Macie détecte des données sensibles dans un objet S3, Macie génère une constatation pour vous informer des données sensibles détectées.

Outre les résultats, Macie fournit des statistiques et des informations qui donnent un aperçu du niveau de sécurité de vos données Amazon S3 et de la localisation des données sensibles dans votre parc de données. Les statistiques et informations peuvent vous aider à prendre des décisions pour effectuer des recherches plus approfondies sur des buckets et des objets S3 spécifiques. Vous pouvez consulter et analyser les résultats, les statistiques et d'autres informations à l'aide de la console Amazon Macie ou de l'API Amazon Macie. Vous pouvez également tirer parti de l'intégration de Macie AWS Security Hub à Amazon EventBridge et surveiller, traiter et corriger les résultats en utilisant d'autres services, applications et systèmes.

Rubriques

Caractéristiques d'Amazon Macie

Voici quelques-unes des principales manières dont Amazon Macie peut vous aider à découvrir, surveiller et protéger vos données sensibles dans Amazon S3.

Automatisez la découverte de données sensibles

Avec Macie, vous pouvez automatiser la découverte et le reporting des données sensibles de deux manières : en configurant Macie pour effectuer la découverte automatique des données sensibles, et en créant et en exécutant des tâches de découverte de données sensibles. Si Macie détecte des données sensibles dans un objet S3, il crée une recherche de données sensibles pour vous. La découverte fournit un rapport détaillé des données sensibles détectées par Macie.

La découverte automatisée des données sensibles fournit une visibilité étendue sur l'emplacement des données sensibles susceptibles de se trouver dans votre parc de données Amazon S3. Avec cette option, Macie évalue en permanence votre inventaire de compartiments S3 et utilise des techniques d'échantillonnage pour identifier et sélectionner des objets S3 représentatifs de vos compartiments. Macie récupère et analyse ensuite les objets sélectionnés, en les inspectant pour détecter la présence de données sensibles.

Les tâches de découverte de données sensibles permettent une analyse plus approfondie et plus ciblée. Avec cette option, vous définissez l'étendue et la profondeur de l'analyse : les compartiments S3 à analyser, la profondeur d'échantillonnage et les critères personnalisés dérivés des propriétés des objets S3. Vous pouvez également configurer une tâche pour qu'elle ne soit exécutée qu'une seule fois pour une analyse et une évaluation à la demande, ou de manière récurrente pour une analyse, une évaluation et une surveillance périodiques.

Les deux options peuvent vous aider à créer et à conserver une vue complète des données que votre organisation stocke dans Amazon S3 et des risques de sécurité ou de conformité associés à ces données.

Découvrez une variété de types de données sensibles

Pour découvrir des données sensibles avec Macie, vous pouvez utiliser des critères et des techniques intégrés, tels que l'apprentissage automatique et la correspondance de modèles, pour analyser des objets dans des compartiments S3. Ces critères et techniques, appelés identifiants de données gérés, permettent de détecter une liste importante et croissante de types de données sensibles pour de nombreux pays et régions, notamment plusieurs types d'informations personnelles identifiables (PII), d'informations financières et de données d'identification.

Vous pouvez également utiliser des identifiants de données personnalisés. Un identifiant de données personnalisé est un ensemble de critères que vous définissez pour détecter les données sensibles : une expression régulière (regex) qui définit un modèle de texte correspondant et, éventuellement, des séquences de caractères et une règle de proximité qui affinent les résultats. Avec ce type d'identifiant, vous pouvez détecter les données sensibles qui reflètent vos scénarios particuliers, votre propriété intellectuelle ou vos données propriétaires. Vous pouvez compléter les identifiants de données gérés fournis par Macie.

Pour affiner les analyses, vous pouvez également utiliser des listes d'autorisations. Les listes d'autorisation définissent le texte et les modèles de texte spécifiques que vous souhaitez que Macie ignore dans les objets S3. Il s'agit généralement d'exceptions relatives aux données sensibles correspondant à vos scénarios ou à votre environnement particuliers, par exemple les noms des représentants publics de votre organisation, les numéros de téléphone publics de votre organisation ou des exemples de données que votre organisation utilise pour les tests.

Évaluez et surveillez les données à des fins de sécurité et de contrôle d'accès

Lorsque vous activez Macie, Macie génère automatiquement et commence à tenir à jour un inventaire complet de vos compartiments S3 à usage général. Macie commence également à évaluer et à surveiller les compartiments à des fins de sécurité et de contrôle d'accès. Si Macie détecte un problème potentiel lié à la sécurité ou à la confidentialité d'un bucket, il crée une politique pour vous.

Outre les résultats spécifiques, un tableau de bord vous donne un aperçu des statistiques agrégées relatives à vos données Amazon S3. Cela inclut les statistiques relatives à des indicateurs clés tels que le nombre de compartiments accessibles au public ou partagés avec d'autres Comptes AWS personnes. Vous pouvez effectuer une analyse détaillée de chaque statistique pour consulter les données justificatives.

Macie fournit également des informations détaillées et des statistiques pour les différents compartiments S3 de votre inventaire. Les données incluent le détail des paramètres d'accès public et de chiffrement d'un compartiment, ainsi que la taille et le nombre d'objets que Macie peut analyser pour détecter les données sensibles contenues dans le compartiment. Vous pouvez parcourir l'inventaire ou le trier et le filtrer en fonction de certains champs.

Examiner et analyser les résultats

Dans Macie, une découverte est un rapport détaillé des données sensibles détectées par Macie dans un objet S3 ou un problème potentiel lié à la sécurité ou à la confidentialité d'un compartiment S3 à usage général. Chaque résultat fournit une note de gravité, des informations

sur la ressource affectée et des détails supplémentaires, tels que le moment et la manière dont Macie a détecté les données ou le problème.

Pour consulter, analyser et gérer les résultats, vous pouvez utiliser les pages Résultats de la console Amazon Macie. Ces pages répertorient vos résultats et fournissent les détails de chaque résultat. Ils proposent également plusieurs options pour regrouper, filtrer, trier et supprimer les résultats. Vous pouvez également utiliser l'API Amazon Macie pour interroger, récupérer et supprimer les résultats. Si vous utilisez l'API, vous pouvez transmettre les données à une autre application, à un autre service ou à un autre système pour une analyse plus approfondie, un stockage à long terme ou des rapports.

Surveiller et traiter les résultats avec d'autres services et systèmes

Pour faciliter l'intégration avec d'autres services et systèmes, Macie publie ses résultats sur Amazon EventBridge sous forme d'événements de recherche. EventBridge est un service de bus d'événements sans serveur qui peut acheminer les données de résultats vers des cibles telles que des AWS Lambda fonctions et des rubriques Amazon Simple Notification Service (Amazon SNS). Vous pouvez ainsi surveiller et traiter les résultats en temps quasi réel dans le cadre de vos flux de travail existants en matière de sécurité et de conformité. EventBridge

Vous pouvez configurer Macie pour qu'il publie également les résultats sur. AWS Security Hub Security Hub est un service qui fournit une vue complète de votre niveau de sécurité dans l'ensemble de votre AWS environnement et vous aide à vérifier que votre environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité. Security Hub vous permet de surveiller et de traiter plus facilement vos résultats dans le cadre d'une analyse plus large du niveau de sécurité de votre entreprise dans AWS. Vous pouvez également agréger les résultats de plusieurs Régions AWS, puis surveiller et traiter les données de résultats agrégées provenant d'une seule région.

Gérez de manière centralisée plusieurs comptes Macie

Si votre AWS environnement comporte plusieurs comptes, vous pouvez gérer Macie de manière centralisée pour les comptes de votre environnement. Vous pouvez le faire de deux manières : en intégrant Macie à Macie AWS Organizations ou en envoyant et en acceptant des invitations d'adhésion dans Macie.

Dans une configuration à comptes multiples, un administrateur Macie désigné peut effectuer certaines tâches et accéder à certains paramètres, données et ressources Macie pour les comptes membres de la même organisation. Les tâches incluent l'examen des informations relatives aux compartiments S3 détenus par les comptes des membres, l'examen des conclusions

des politiques relatives à ces compartiments et l'inspection des compartiments pour détecter la présence de données sensibles dans les compartiments. Si les comptes sont associés via AWS Organizations, l'administrateur Macie peut également activer Macie pour les comptes des membres de l'organisation.

Développer et gérer les ressources de manière programmatique

Outre la console Amazon Macie, vous pouvez interagir avec Macie à l'aide de l'API Amazon Macie. L'API Amazon Macie vous donne un accès complet et programmatique aux paramètres, aux données et aux ressources de votre compte Macie.

Pour interagir avec Macie par programmation, vous pouvez envoyer des requêtes HTTPS directement à Macie ou utiliser une version actuelle d'un outil de ligne de AWS commande ou d'un SDK. AWS AWS fournit des outils et des SDK composés de bibliothèques et d'exemples de code pour différents langages et plateformes PowerShell, tels que Java, Go, Python, C++ et .NET.

Accès à Amazon Macie

Amazon Macie est disponible dans la plupart des pays. Régions AWS Pour obtenir la liste des régions dans lesquelles Macie est actuellement disponible, consultez la section Points de terminaison et quotas Amazon Macie dans le. Références générales AWS Pour plus d'informations sur la gestion Régions AWS de votre compte Compte AWS, voir Spécifier les comptes que Régions AWS votre compte peut utiliser dans le Guide de AWS Account Management référence.

Dans chaque région, vous pouvez travailler avec Macie de l'une des manières suivantes.

AWS Management Console

AWS Management Console Il s'agit d'une interface basée sur un navigateur que vous pouvez utiliser pour créer et gérer AWS des ressources. Dans le cadre de cette console, la console Amazon Macie permet d'accéder à votre compte Macie, à vos données et à vos ressources. Vous pouvez effectuer n'importe quelle tâche Macie à l'aide de la console Macie : consultez les statistiques et autres informations relatives à vos compartiments S3, créez et exécutez des tâches de découverte de données sensibles, consultez et analysez les résultats, etc.

AWS outils de ligne de commande

Avec les outils de ligne de AWS commande, vous pouvez émettre des commandes sur la ligne de commande de votre système pour effectuer des tâches et AWS des tâches Macie. L'utilisation

de la ligne de commande peut être plus rapide et plus pratique que celle de la console. Les outils de ligne de commande sont également utiles si vous souhaitez créer des scripts exécutant des tâches .

AWS fournit deux ensembles d'outils de ligne de commande : le AWS Command Line Interface (AWS CLI) et le AWS Tools for PowerShell. Pour plus d'informations sur l'installation et l'utilisation du AWS CLI, consultez le guide de AWS Command Line Interface l'utilisateur. Pour plus d'informations sur l'installation et l'utilisation des outils pour PowerShell, consultez le guide de AWS Tools for PowerShell l'utilisateur.

AWS Kits SDK

AWS fournit des SDK composés de bibliothèques et d'exemples de code pour différents langages de programmation et plateformes, par exemple Java, Go, Python, C++ et .NET. Les SDK fournissent un accès pratique et programmatique à Macie et à d'autres. Services AWS Ils gèrent également des tâches telles que la signature cryptographique des demandes, la gestion des erreurs et le renouvellement automatique des demandes. Pour plus d'informations sur l'installation et l'utilisation des AWS SDK, consultez la section Outils sur AWS lesquels vous pouvez vous appuyer.

API REST Amazon Macie

L'API REST Amazon Macie vous donne un accès complet et programmatique à votre compte, à vos données et à vos ressources Macie. Avec cette API, vous pouvez envoyer des requêtes HTTPS directement à Macie. Cependant, contrairement aux outils de ligne de AWS commande et aux SDK, l'utilisation de cette API nécessite que votre application gère des détails de bas niveau tels que la génération d'un hachage pour signer une demande. Pour plus d'informations sur cette API, consultez le manuel Amazon Macie API Reference.

Tarification pour Amazon Macie

Comme pour les autres AWS produits, il n'existe aucun contrat ou engagement minimum pour utiliser Amazon Macie.

La tarification de Macie repose sur plusieurs dimensions : évaluation et surveillance des compartiments S3 pour la sécurité et le contrôle d'accès, surveillance des objets S3 pour la découverte automatique des données sensibles et analyse des objets S3 pour découvrir et signaler les données sensibles contenues dans les objets. Pour plus d'informations, consultez les tarifs d'Amazon Macie.

Pour vous aider à comprendre et à prévoir le coût d'utilisation de Macie, Macie fournit une estimation des coûts d'utilisation de votre compte. Vous pouvez consulter ces estimations sur la console Amazon Macie et y accéder via l'API Amazon Macie. Selon la manière dont vous utilisez le service, l'utilisation d'autres Services AWS fonctionnalités associées à certaines fonctionnalités de Macie peut entraîner des coûts supplémentaires, telles que la récupération des données des compartiments depuis Amazon S3 et l'utilisation d'une solution gérée par le client AWS KMS keys pour déchiffrer des objets à des fins d'analyse.

Lorsque vous activez Macie pour la première fois, vous êtes automatiquement Compte AWS inscrit à l'essai gratuit de 30 jours de Macie. Cela inclut les comptes individuels activés dans le cadre d'une organisation dans AWS Organizations. Pendant l'essai gratuit, l'utilisation de Macie dans le cas applicable est gratuite pour évaluer et surveiller vos compartiments S3 Région AWS à des fins de sécurité et de contrôle d'accès. En fonction des paramètres de votre compte, l'essai gratuit peut également inclure la découverte automatique de données sensibles pour vos données Amazon S3. L'essai gratuit n'inclut pas l'exécution de tâches de découverte de données sensibles pour découvrir et signaler des données sensibles dans des objets S3.

Pour vous aider à comprendre et à prévoir le coût d'utilisation de Macie après la fin de l'essai gratuit, Macie vous fournit une estimation des coûts d'utilisation en fonction de votre utilisation de Macie pendant la période d'essai. Vos données d'utilisation indiquent également le temps qu'il reste avant la fin de votre essai gratuit. Vous pouvez consulter ces données sur la console Amazon Macie et y accéder via l'API Amazon Macie.

Services connexes

Pour renforcer la sécurité de vos données, de vos charges de travail et de vos applications AWS, pensez à utiliser les solutions suivantes Services AWS en combinaison avec Amazon Macie.

AWS Security Hub

> AWS Security Hub vous donne une vue complète de l'état de sécurité de vos AWS ressources et vous aide à vérifier que votre AWS environnement est conforme aux normes du secteur de la sécurité et aux meilleures pratiques. Pour ce faire, il utilise, agrège, organise et hiérarchise les résultats de sécurité provenant de multiples produits Services AWS (y compris Macie) et du réseau de AWS partenaires (APN) pris en charge. Security Hub vous aide à analyser les tendances en matière de sécurité et à identifier les problèmes de sécurité les plus prioritaires dans votre AWS environnement.

Pour en savoir plus sur Security Hub, consultez le guide de AWS Security Hub l'utilisateur. Pour en savoir plus sur l'utilisation conjointe de Macie et Security Hub, consultezIntégration d'Amazon Macie avec AWS Security Hub.

Amazon GuardDuty

Amazon GuardDuty est un service de surveillance de la sécurité qui analyse et traite certains types de AWS journaux, tels que les journaux d'événements de AWS CloudTrail données pour Amazon S3 et les journaux d'événements CloudTrail de gestion. Il utilise des flux de renseignements sur les menaces, tels que des listes d'adresses IP et de domaines malveillants, et l'apprentissage automatique pour identifier les activités inattendues, potentiellement non autorisées et malveillantes au sein de votre AWS environnement.

Pour en savoir plus GuardDuty, consultez le guide de GuardDuty l'utilisateur Amazon.

Pour en savoir plus sur les services AWS de sécurité supplémentaires, consultez la section Sécurité, identité et conformité sur AWS.

Commencer à utiliser Amazon Macie

Ce didacticiel fournit une introduction à Amazon Macie. Vous allez apprendre comment activer Macie pour votre Compte AWS. Vous apprendrez également à évaluer votre niveau de sécurité avec Amazon Simple Storage Service (Amazon S3) et à configurer les principaux paramètres et ressources pour découvrir et signaler les données sensibles dans vos compartiments S3.

Tâches

Avant de commencer

Lorsque vous vous inscrivez à Amazon Web Services (AWS), votre compte est automatiquement ouvert à tous Services AWS, y compris Amazon Macie. Toutefois, pour activer et utiliser Macie, vous devez d'abord configurer des autorisations vous permettant d'accéder à la console Amazon Macie et aux opérations de l'API. Vous ou votre AWS administrateur pouvez le faire en utilisant AWS Identity and Access Management (IAM) pour associer la politique AWS gérée nommée `AmazonMacieFullAccess` à votre identité IAM. Pour en savoir plus, veuillez consulter la section AWSpolitiques gérées pour Amazon Macie.

Étape 1 : activer Amazon Macie

Après avoir configuré les autorisations requises, vous pouvez activer Amazon Macie pour votre. Compte AWS Suivez ces étapes pour activer Macie pour votre compte.

Pour activer Macie

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez activer et utiliser Macie.

3. Sur la page Amazon Macie, choisissez Get started.
4. (Facultatif) Lorsque vous activez Macie, Macie crée automatiquement un rôle lié à un service qui accorde à Macie les autorisations nécessaires pour appeler d'autres ressources Services AWS et surveiller AWS les ressources en votre nom. Pour consulter la politique d'autorisation pour ce rôle, choisissez Afficher les autorisations du rôle sur la console. Pour de plus amples informations sur ce rôle, veuillez consulter Rôles liés à un service pour Amazon Macie.
5. Choisissez Enable Macie (Activer Macie).

En quelques minutes, Macie génère et commence automatiquement à tenir à jour un inventaire complet de vos compartiments S3 à usage général dans la région actuelle. Macie commence également à évaluer et à surveiller les compartiments à des fins de sécurité et de contrôle d'accès. Pour en savoir plus, veuillez consulter la section Comment Macie surveille la sécurité des données Amazon S3.

En fonction des paramètres de votre compte, Macie commence également à effectuer une découverte automatique des données sensibles pour vos compartiments S3. Macie commence à identifier, sélectionner et analyser en permanence les objets représentatifs de vos compartiments, en inspectant ces objets pour détecter la présence de données sensibles. Au fur et à mesure que les analyses progressent, Macie fournit des statistiques et d'autres résultats que vous pouvez consulter, généralement dans les 48 heures suivant l'activation de Macie pour votre compte. Vous pouvez personnaliser les analyses en configurant les paramètres de découverte automatique des données sensibles pour votre compte. Pour en savoir plus, veuillez consulter la section Comment fonctionne la découverte automatique des données sensibles.

Pour consulter les statistiques agrégées de vos données Amazon S3, choisissez Summary dans le volet de navigation de la console. Pour consulter les informations relatives aux compartiments S3 individuels de votre inventaire, sélectionnez les compartiments S3 dans le volet de navigation. Pour afficher ensuite les détails d'un bucket, choisissez-le. Le panneau de détails affiche des statistiques et d'autres informations qui fournissent un aperçu de la sécurité, de la confidentialité et de la sensibilité des données du bucket. Pour en savoir plus sur ces détails, consultezRévision de l'inventaire de votre compartiment S3.

Étape 2 : Configuration d'un référentiel pour les résultats de découverte de données sensibles

Avec Amazon Macie, vous pouvez découvrir des données sensibles dans vos compartiments S3 de deux manières : en configurant Macie pour qu'il effectue une découverte automatique des données sensibles et en exécutant des tâches de découverte de données sensibles. Une tâche de découverte de données sensibles est une tâche que vous créez pour analyser des objets dans des compartiments S3 afin de déterminer s'ils contiennent des données sensibles.

Macie crée un enregistrement pour chaque objet S3 qu'il analyse lorsque vous exécutez des tâches de découverte de données sensibles ou lorsqu'il effectue une découverte automatique de données sensibles. Ces enregistrements, appelés résultats de découverte de données sensibles, contiennent des informations sur l'analyse d'objets individuels. Macie crée également des résultats de découverte de données sensibles pour des objets qu'il ne peut pas analyser en raison d'erreurs ou de problèmes. Les résultats de découverte de données sensibles vous fournissent des enregistrements d'analyse qui peuvent être utiles pour les audits ou les enquêtes sur la confidentialité et la protection des données.

Macie conserve les résultats de la découverte de vos données sensibles pendant 90 jours seulement. Pour accéder aux résultats et permettre leur stockage et leur conservation à long terme, configurez Macie pour qu'il les stocke dans un compartiment S3. Vous devez le faire dans les 30 jours suivant l'activation de Macie. Ensuite, le bucket peut servir de référentiel définitif à long terme pour tous les résultats de découverte de données sensibles.

Pour savoir comment configurer ce référentiel, consultezStockage et conservation des résultats de découverte de données sensibles.

Étape 3 : Explorez les résultats des échantillons

Dans Amazon Macie, il existe deux catégories de conclusions : les conclusions relatives aux politiques et les conclusions relatives aux données sensibles. Macie crée une recherche de politique lorsque les politiques ou les paramètres d'un compartiment à usage général S3 sont modifiés d'une manière qui réduit la sécurité ou la confidentialité du compartiment et de ses objets. Macie crée une recherche de données sensibles lorsqu'il détecte des données sensibles dans un objet S3. Dans chaque catégorie, il existe plusieurs types de résultats.

Pour explorer et découvrir les différentes catégories et types de résultats fournis par Macie, créez et examinez éventuellement des exemples de résultats. Les exemples de résultats utilisent des

exemples de données et des valeurs d'espace réservé pour démontrer le type d'informations que Macie peut inclure dans chaque type de résultat.

Suivez ces étapes pour créer et examiner des exemples de résultats.

Pour créer et examiner des exemples de résultats

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sous Exemples de résultats, choisissez Générer des exemples de résultats. Macie génère un échantillon de résultat pour chaque type de résultat pris en charge par Macie.
4. Dans le volet de navigation, choisissez Conclusions. La page Résultats affiche les résultats actuels relatifs à votre compte Région AWS. Cela inclut les exemples de résultats que vous avez créés à l'étape précédente.
5. Sur la page Résultats, recherchez les résultats dont le type commence par [SAMPLE].
6. Pour consulter les détails d'un résultat d'échantillonnage en particulier, choisissez le résultat. Le panneau de détails affiche les détails de la recherche.

Pour en savoir plus sur chaque type de résultat, voirTypes de résultat. Pour en savoir plus sur la création et la révision d'échantillons de résultats, voirUtilisation des résultats d'échantillons.

Étape 4 : Créez une tâche pour découvrir des données sensibles

Pour découvrir et signaler des données sensibles dans des compartiments S3, vous pouvez exécuter des tâches de découverte de données sensibles. Une tâche de découverte de données sensibles est une tâche que vous créez pour analyser des objets dans des compartiments S3 afin de déterminer s'ils contiennent des données sensibles. Contrairement à la découverte automatique des données sensibles, vous définissez l'étendue et la profondeur de l'analyse. Vous spécifiez également la fréquence d'exécution d'une tâche : une fois ou périodiquement sur une base planifiée.

Procédez comme suit pour créer une tâche qui ne s'exécute qu'une seule fois, immédiatement après sa création, et qui utilise les paramètres par défaut. Pour savoir comment créer une tâche exécutée périodiquement ou utilisant des paramètres personnalisés, consultezCréation d'une tâche de découverte de données sensibles.

Pour créer une tâche de découverte de données sensibles

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.

2. Dans le volet de navigation, sélectionnez Tâches.
3. Choisissez Créer une tâche.
4. Pour l'étape Choisir des compartiments S3, choisissez Sélectionner des compartiments spécifiques. Dans le tableau, cochez ensuite la case correspondant à chaque compartiment S3 que vous souhaitez que la tâche analyse.

   Le tableau fournit un inventaire complet de vos compartiments S3 à usage général actuels Région AWS. Pour trouver plus facilement des compartiments spécifiques, entrez les critères de filtre dans la zone de filtre située au-dessus du tableau. Vous pouvez également trier le tableau en choisissant un titre de colonne dans le tableau.
5. Lorsque vous avez fini de sélectionner les compartiments, choisissez Next.
6. Pour l'étape Réviser les compartiments S3, passez en revue et vérifiez vos sélections de compartiments, puis choisissez Next.
7. Pour l'étape Affiner le champ d'application, choisissez Tâche unique, puis cliquez sur Suivant.
8. Pour l'étape Sélectionner les identifiants de données gérés, choisissez Recommandé. Consultez éventuellement le tableau des identifiants de données gérés que nous recommandons pour les tâches, puis choisissez Next.

   Un identifiant de données géré est un ensemble de critères et de techniques intégrés conçus pour détecter un type spécifique de données sensibles, par exemple les numéros de carte de crédit, les clés d'accès AWS secrètes ou les numéros de passeport d'un pays ou d'une région en particulier. Pour en savoir plus, veuillez consulter la section Utilisation des identificateurs de données gérés.
9. Pour l'étape Sélectionner des identifiants de données personnalisés, choisissez Next.

   Un identifiant de données personnalisé est un ensemble de critères que vous définissez pour détecter les données sensibles : une expression régulière (regex) qui définit un modèle de texte correspondant et, éventuellement, des séquences de caractères et une règle de proximité qui affinent les résultats. Pour en savoir plus, veuillez consulter la section Création d'identificateurs de données personnalisés.
10. Pour l'étape Sélectionner les listes d'autorisation, choisissez Next.

    Dans Macie, une liste d'autorisation indique le texte ou un modèle de texte que vous souhaitez que Macie ignore lorsqu'il inspecte des objets S3 pour détecter la présence de données sensibles. Il s'agit généralement d'exceptions relatives aux données sensibles pour des

scénarios ou des environnements particuliers. Pour en savoir plus, veuillez consulter la section Définition des exceptions relatives aux données sensibles à l'aide de listes d'autorisation.

11. Pour l'étape Entrer les paramètres généraux, entrez un nom et, éventuellement, une description de la tâche. Ensuite, sélectionnez Suivant.
12. Pour l'étape Révision et création, passez en revue les paramètres de configuration de la tâche et vérifiez qu'ils sont corrects.

    Vous pouvez également consulter le coût total estimé (en dollars américains) de l'exécution de la tâche. L'estimation peut vous aider à déterminer s'il convient d'ajuster les paramètres de la tâche avant de l'enregistrer. Pour en savoir plus, veuillez consulter la section Prévision du coût d'une tâche de découverte de données sensibles.
13. Lorsque vous avez terminé de vérifier et de vérifier les paramètres de la tâche, choisissez Soumettre.

Macie commence immédiatement à exécuter le travail. Pour savoir comment surveiller la tâche, consultez la section Vérification de l'état des tâches de découverte de données sensibles.

Étape 5 : Passez en revue vos résultats

Amazon Macie surveille automatiquement la sécurité et le contrôle d'accès de vos compartiments S3 à usage général, et établit des politiques pour signaler les problèmes potentiels liés à la sécurité ou à la confidentialité des compartiments. Si vous exécutez une tâche de découverte de données sensibles ou si vous configurez Macie pour effectuer une découverte automatique de données sensibles, Macie crée des résultats de données sensibles pour signaler les données sensibles détectées dans les objets S3. Pour en savoir plus sur les résultats, veuillez consulter Analyse des résultats.

Suivez ces étapes pour passer en revue vos résultats.

Pour passer en revue vos résultats

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Conclusions. La page Résultats affiche les résultats actuels relatifs à votre compte Région AWS.
3. (Facultatif) Pour filtrer les résultats selon des critères spécifiques, entrez les critères dans le champ de filtre situé au-dessus du tableau.

4. Pour consulter les détails d'un résultat en particulier, choisissez-le. Le panneau de détails affiche les détails de la recherche.

Pour en savoir plus, notamment sur la façon de regrouper et de filtrer les résultats, voirExamen des résultats.

Concepts et terminologie d'Amazon Macie

Dans Amazon Macie, nous nous appuyons sur des AWS concepts et une terminologie courants et utilisons ces termes supplémentaires.

compte

Une norme Compte AWS qui contient vos AWS ressources et les identités qui peuvent accéder à ces ressources.

Pour utiliser Macie, vous devez vous connecter à l' AWS aide de vos Compte AWS informations d'identification, sélectionner celle Région AWS dans laquelle vous souhaitez utiliser Macie, puis activer Macie pour vous Compte AWS dans cette région. Pour plus d'informations, consultez Commencer à utiliser Amazon Macie.

Il existe trois types de comptes dans Macie :

- Compte administrateur — Ce type de compte gère les comptes Macie d'une organisation. Une organisation est un ensemble de comptes Macie associés les uns aux autres et gérés de manière centralisée en tant que groupe de comptes associés au sein d'un groupe spécifique Région AWS.
- Compte membre — Ce type de compte est associé et géré par le compte administrateur Macie d'une organisation.
- Compte autonome — Ce type de compte n'est ni un compte administrateur ni un compte membre. Il ne fait pas partie d'une organisation.

Vous pouvez ajouter des comptes Macie à une organisation de deux manières : en intégrant Macie à Macie AWS Organizations ou en envoyant et en acceptant des invitations d'adhésion à Macie. Pour plus d'informations, consultez Gestion de plusieurs comptes .

compte administrateur

Dans Macie, compte qui gère les comptes Macie d'une organisation. Une organisation est un ensemble de comptes Macie associés les uns aux autres et gérés de manière centralisée en tant que groupe de comptes associés au sein d'un groupe spécifique Région AWS.

Les utilisateurs d'un compte administrateur Macie ont accès aux données d'inventaire d'Amazon Simple Storage Service (Amazon S3), aux conclusions des politiques, ainsi qu'à certains paramètres

et ressources Macie pour tous les comptes de leur organisation. Ils peuvent également effectuer une découverte automatique des données sensibles et exécuter des tâches de découverte de données sensibles pour détecter les données sensibles dans les compartiments S3 détenus par les comptes. Selon la manière dont un compte est désigné en tant que compte administrateur, ils peuvent également être en mesure d'effectuer des tâches supplémentaires pour d'autres comptes de leur organisation.

Pour plus d'informations, consultez Gestion de plusieurs comptes .

liste d'autorisation

Dans Macie, une liste d'autorisation indique le texte ou un modèle de texte que vous souhaitez que Macie ignore lorsqu'il inspecte des objets S3 pour détecter la présence de données sensibles.

Vous pouvez créer deux types de listes d'autorisation dans Macie : un fichier en texte brut qui répertorie des mots spécifiques et d'autres types de séquences de caractères à ignorer, ou une expression régulière (regex) qui définit un modèle de texte à ignorer. Si un objet contient du texte correspondant à une entrée ou à un modèle d'une liste d'autorisation, Macie n'indique pas le texte dans les résultats relatifs aux données sensibles, les statistiques et les autres types de résultats, même si le texte répond aux critères d'un identifiant de données géré ou d'un identifiant de données personnalisé.

Pour plus d'informations, consultez Définition des exceptions relatives aux données sensibles à l'aide de listes d'autorisation.

découverte automatisée des données sensibles

Série d'activités d'analyse automatisées que Macie effectue en permanence pour identifier et sélectionner des objets représentatifs dans des compartiments S3, et inspecter les objets sélectionnés pour détecter la présence de données sensibles.

Au fur et à mesure que les analyses progressent, Macie produit des enregistrements des données sensibles qu'elle trouve (résultats de découverte de données sensibles) et de l'analyse qu'elle effectue (résultats de découverte de données sensibles). Macie met également à jour les statistiques et les autres informations qu'il fournit sur les données Amazon S3.

Pour plus d'informations, consultez Réalisation de la découverte automatisée des données sensibles.

AWS Format de recherche de sécurité (ASFF)

Format JSON standardisé pour le contenu des résultats publiés ou générés par AWS Security Hub. L'ASFF inclut des informations sur la source d'un problème de sécurité, les ressources concernées et l'état d'une découverte.

Pour plus d'informations sur ASFF, voir AWS Security Finding Format (ASFF) dans le guide de l'AWS Security Hub utilisateur. Pour plus d'informations sur la publication des résultats de Macie sur Security Hub, consultezIntégration d'Amazon Macie avec AWS Security Hub.

octets ou taille classifiables

Dans les statistiques du compartiment S3 fournies par Macie, la taille de stockage totale de tous les objets classifiables d'un compartiment S3.

Si le versionnement est activé pour un compartiment, cette valeur est basée sur la taille de stockage de la dernière version de chaque objet classifiable du compartiment. Si un objet est un fichier compressé, cette valeur ne reflète pas la taille réelle du contenu du fichier une fois celui-ci décompressé.

Pour plus d'informations, consultez Révision de l'inventaire de votre compartiment S3 et Évaluation du niveau de sécurité de votre Amazon S3.

objet classifiable

Un objet S3 que Macie peut analyser pour détecter des données sensibles.

Lors du calcul des statistiques du compartiment S3, Macie détermine qu'un objet est classable en fonction de sa classe de stockage et de son extension de nom de fichier. Un objet est classifiable s'il utilise une classe de stockage Amazon S3 prise en charge et possède une extension de nom de fichier pour un format de fichier ou de stockage pris en charge.

Pour plus d'informations, consultez Révision de l'inventaire de votre compartiment S3 et Évaluation du niveau de sécurité de votre Amazon S3.

Pour la découverte de données sensibles, Macie détermine qu'un objet est classifiable en fonction de sa classe de stockage, de son extension de nom de fichier et de son contenu. Un objet est

classifiable s'il utilise une classe de stockage Amazon S3 prise en charge, s'il possède une extension de nom de fichier pour un format de fichier ou de stockage pris en charge, et Macie a vérifié qu'il peut extraire et analyser les données de l'objet.

Pour plus d'informations, consultez Découverte de données sensibles et Prévision et surveillance des coûts.

identifiant de données personnalisé

Ensemble de critères que vous définissez pour détecter les données sensibles.

Les critères sont constitués d'une expression régulière (regex) qui définit un modèle de texte à mettre en correspondance et, éventuellement, des séquences de caractères et une règle de proximité qui affinent les résultats. Les séquences de caractères peuvent être :

- des mots-clés, qui sont des mots ou des phrases qui doivent se trouver à proximité du texte qui correspond à la regex, ou
- des mots à ignorer, qui sont des mots ou des phrases à exclure des résultats.

Outre les critères de détection, vous pouvez définir des paramètres de gravité personnalisés pour les résultats de données sensibles produits par un identifiant de données personnalisé.

Pour plus d'informations, consultez Création d'identificateurs de données personnalisés.

règle de filtrage

Ensemble de critères de filtrage basés sur des attributs que vous créez et enregistrez pour analyser les résultats sur la console Amazon Macie. Les règles de filtrage peuvent vous aider à effectuer une analyse cohérente des résultats présentant des caractéristiques spécifiques, tels que tous les résultats très graves qui signalent un type spécifique de données sensibles.

Pour plus d'informations, consultez Création et gestion de règles de filtrage pour les résultats.

résultat

Rapport détaillé des données sensibles trouvées par Macie dans un objet S3 ou d'un problème potentiel lié à la sécurité ou à la confidentialité d'un compartiment S3 à usage général. Chaque

résultat fournit des détails tels qu'une note de gravité, des informations sur la ressource affectée et la date à laquelle Macie a découvert les données ou le problème.

Macie génère deux catégories de résultats : les résultats relatifs aux données sensibles, pour les données sensibles détectées par Macie dans les objets S3, et les résultats relatifs aux politiques, concernant les problèmes potentiels détectés par Macie dans les paramètres de sécurité et de contrôle d'accès des compartiments S3. Dans chaque catégorie, il existe des types spécifiques de résultats.

Pour plus d'informations, consultez Types de résultats sur Amazon Macie.

recherche d'un événement

Un EventBridge événement Amazon qui contient les détails d'une découverte de données sensibles ou d'une constatation de politique.

Macie publie automatiquement les résultats relatifs aux données sensibles et aux politiques sur Amazon EventBridge sous forme d'événements. Un événement est un objet JSON conforme au EventBridge schéma des AWS événements. Vous pouvez utiliser ces événements pour surveiller, traiter et agir en fonction des résultats en utilisant d'autres applications, services et systèmes.

Pour plus d'informations, consultez Intégration d'Amazon Macie à Amazon EventBridge et Schéma EventBridge d'événement Amazon pour les résultats d'Amazon Macie.

tâche

Voir le travail de découverte de données sensibles.

identifiant de données gérées

Ensemble de critères et de techniques intégrés conçus pour détecter un type spécifique de données sensibles. Les numéros de carte de crédit, les clés d'accès AWS secrètes ou les numéros de passeport d'un pays ou d'une région en particulier sont des exemples de données sensibles. Ces identifiants peuvent détecter une liste longue et croissante de types de données sensibles pour de nombreux pays et régions.

Pour plus d'informations, consultez Utilisation des identificateurs de données gérés.

compte membre

Un compte Macie géré par le compte administrateur Macie désigné pour une organisation. Une organisation est un ensemble de comptes Macie associés les uns aux autres et gérés de manière centralisée en tant que groupe de comptes associés au sein d'un groupe spécifique Région AWS.

Un compte peut devenir un compte membre de deux manières : en intégrant Macie à l'organisation du compte AWS Organizations ou en acceptant une invitation d'adhésion à Macie.

Si vous avez un compte membre, votre administrateur Macie a accès aux données d'inventaire Amazon S3, aux conclusions des politiques, ainsi qu'à certains paramètres et ressources Macie pour votre compte. Votre administrateur peut également effectuer une découverte automatique des données sensibles et exécuter des tâches de découverte de données sensibles pour détecter les données sensibles dans vos compartiments S3. Ils peuvent également être en mesure d'effectuer des tâches supplémentaires pour votre compte, en fonction de la façon dont votre compte est devenu un compte de membre.

Pour plus d'informations, consultez Gestion de plusieurs comptes .

organization

Ensemble de comptes Macie associés les uns aux autres et gérés de manière centralisée en tant que groupe de comptes associés au sein d'un groupe spécifique Région AWS.

Chaque organisation se compose d'un compte administrateur Macie désigné et d'un ou plusieurs comptes de membres associés. Le compte administrateur peut accéder à certains paramètres, données et ressources Macie pour les comptes des membres. Vous pouvez créer une organisation de deux manières : en intégrant Macie à Macie AWS Organizations ou en envoyant et en acceptant des invitations d'adhésion dans Macie.

Pour plus d'informations, consultez Gestion de plusieurs comptes .

constatation d'une politique

Rapport détaillé d'une violation potentielle des politiques ou d'un problème lié aux paramètres de sécurité et de contrôle d'accès d'un compartiment S3 à usage général. Les détails incluent une note de gravité, des informations sur la ressource affectée et la date à laquelle Macie a découvert le problème.

Macie génère des conclusions relatives aux politiques lorsque les politiques ou les paramètres d'un compartiment à usage général S3 sont modifiés de manière à réduire la sécurité ou la confidentialité du compartiment et de ses objets. Macie génère ces résultats dans le cadre de ses activités de surveillance continue de vos données Amazon S3. Macie peut générer plusieurs types de conclusions politiques.

Pour plus d'informations, consultez Types de résultats sur Amazon Macie et Surveillance de la sécurité et de la confidentialité des données.

recherche d'échantillons

Un résultat qui utilise des exemples de données et des valeurs d'espace réservé pour démontrer le type d'informations qu'un résultat peut contenir.

Pour plus d'informations, consultez Utilisation des résultats d'échantillons.

recherche de données sensibles

Rapport détaillé des données sensibles que Macie a trouvées dans un objet S3. Les détails incluent une note de gravité, des informations sur la ressource affectée, le type et le nombre d'occurrences des données sensibles trouvées par Macie, et la date à laquelle Macie a trouvé les données sensibles.

Macie génère des résultats de données sensibles s'il détecte des données sensibles dans des objets S3 qu'il analyse lorsque vous exécutez des tâches de découverte de données sensibles ou s'il effectue une découverte automatique de données sensibles. Macie peut générer plusieurs types de résultats de données sensibles.

Pour plus d'informations, consultez Types de résultats sur Amazon Macie et Découverte de données sensibles.

tâche de découverte de données sensibles

Également appelée tâche, une série de tâches de traitement et d'analyse automatisées effectuées par Macie pour détecter et signaler les données sensibles dans les objets S3. Lorsque vous créez une tâche, vous spécifiez la fréquence à laquelle vous souhaitez qu'elle soit exécutée, et vous définissez la portée et la nature de l'analyse de la tâche.

Lorsqu'une tâche est exécutée, Macie enregistre les données sensibles qu'elle trouve (résultats de données sensibles) et l'analyse qu'elle effectue (résultats de découverte de données sensibles). Macie publie également des données de journalisation sur Amazon CloudWatch Logs.

Pour plus d'informations, consultez Exécution de tâches de découverte de données sensibles.

résultat de découverte de données sensibles

Enregistrement qui enregistre les détails de l'analyse effectuée par Macie sur un objet S3 afin de déterminer si l'objet contient des données sensibles. Macie génère et écrit ces enregistrements dans des fichiers JSON Lines (.jsonl), qu'il chiffre et stocke dans un compartiment S3 que vous spécifiez. Les enregistrements sont conformes à un schéma standardisé.

Lorsque vous exécutez une tâche de découverte de données sensibles ou que Macie effectue une découverte automatique de données sensibles, Macie crée un résultat de découverte de données sensibles pour chaque objet inclus dans le périmètre de l'analyse. Cela consiste notamment à :

- Objets dans lesquels Macie trouve des données sensibles et, par conséquent, produisent également des résultats de données sensibles.
- Objets dans lesquels Macie ne trouve pas de données sensibles et ne produisent donc pas de résultats de données sensibles.
- Objets que Macie ne peut pas analyser en raison d'erreurs ou de problèmes tels que les paramètres d'autorisation ou l'utilisation d'un format de fichier ou de stockage non pris en charge.

Pour plus d'informations, consultez Stockage et conservation des résultats de découverte de données sensibles.

compte autonome

Un compte Macie qui n'est ni un compte administrateur ni un compte membre dans une organisation. Le compte ne fait pas partie d'une organisation.

découverte supprimée

Une découverte qui a été archivée automatiquement par une règle de suppression. En d'autres termes, Macie a automatiquement changé le statut du résultat en archivé parce que le résultat correspondait aux critères d'une règle de suppression lorsque Macie a généré le résultat.

Pour plus d'informations, consultez Suppression de résultats.

règle de suppression

Ensemble de critères de filtrage basés sur des attributs que vous créez et enregistrez pour archiver (supprimer) automatiquement les résultats. Les règles de suppression sont utiles lorsque vous avez examiné une catégorie de résultats et que vous ne souhaitez pas en être informé à nouveau.

Si vous supprimez des résultats à l'aide d'une règle de suppression, Macie continue de générer des résultats correspondant aux critères de la règle. Cependant, Macie change automatiquement le statut des résultats en « archivé ». Cela signifie que les résultats n'apparaissent pas par défaut sur la console Amazon Macie et que Macie ne les publie pas sur d'autres plateformes. Services AWS

Pour plus d'informations, consultez Suppression de résultats.

octets ou taille inclassables

Dans les statistiques du compartiment S3 fournies par Macie, la taille de stockage totale de tous les objets inclassables d'un compartiment S3.

Si le versionnement est activé pour un compartiment, cette valeur est basée sur la taille de stockage de la dernière version de chaque objet inclassable du compartiment. Si un objet est un fichier compressé, cette valeur ne reflète pas la taille réelle du contenu du fichier une fois celui-ci décompressé.

Pour plus d'informations, consultez Révision de l'inventaire de votre compartiment S3 et Évaluation du niveau de sécurité de votre Amazon S3.

objet inclassable

Un objet S3 que Macie ne peut pas analyser pour détecter des données sensibles.

Lors du calcul des statistiques du compartiment S3, Macie détermine qu'un objet est inclassable en fonction de sa classe de stockage et de son extension de nom de fichier. Un objet est inclassable s'il n'utilise pas une classe de stockage Amazon S3 prise en charge ou s'il ne possède pas d'extension de nom de fichier pour un format de fichier ou de stockage pris en charge.

Pour plus d'informations, consultez Révision de l'inventaire de votre compartiment S3 et Évaluation du niveau de sécurité de votre Amazon S3.

Pour la découverte de données sensibles, Macie détermine qu'un objet est inclassable en fonction de sa classe de stockage, de son extension de nom de fichier et de son contenu. Un objet est inclassable s'il n'utilise pas de classe de stockage Amazon S3 prise en charge, s'il ne possède pas d'extension de nom de fichier ou de format de stockage pris en charge, ou si Macie n'a pas pu extraire et analyser les données de l'objet. Par exemple, l'objet est un fichier mal formé.

Pour plus d'informations, consultez Découverte de données sensibles et Prévision et surveillance des coûts.

Surveillance de la sécurité et de la confidentialité des données avec Amazon Macie

Lorsque vous activez Amazon Macie pour votre compte Compte AWS, Macie génère et commence automatiquement à gérer un inventaire complet de vos compartiments à usage général Amazon Simple Storage Service (Amazon S3) dans le courant actuel. Région AWS Macie commence également à évaluer et à surveiller les compartiments à des fins de sécurité et de contrôle d'accès. Si Macie détecte un événement qui réduit la sécurité ou la confidentialité d'un bucket, Macie crée une politique que vous pouvez examiner et corriger si nécessaire.

Pour évaluer et surveiller également la présence de données sensibles dans les compartiments S3, vous pouvez créer et exécuter des tâches de découverte de données sensibles. Les tâches de découverte de données sensibles peuvent effectuer une analyse incrémentielle des objets du compartiment sur une base quotidienne, hebdomadaire ou mensuelle. Si Macie détecte des données sensibles dans un objet S3, Macie crée une recherche de données sensibles pour vous informer des données sensibles détectées. En fonction des paramètres de votre compte, vous pouvez également configurer Macie pour effectuer la découverte automatique des données sensibles. La découverte automatisée des données sensibles utilise des techniques d'échantillonnage pour identifier, sélectionner et analyser en permanence des objets représentatifs dans vos compartiments. Pour plus d'informations sur les deux options, consultezDécouverte de données sensibles.

Macie fournit également une visibilité constante sur la sécurité et la confidentialité de vos données Amazon S3. Pour évaluer le niveau de sécurité de vos données et déterminer les mesures à prendre, vous pouvez utiliser le tableau de bord récapitulatif de la console. Le tableau de bord fournit un aperçu des statistiques agrégées pour vos données Amazon S3. Les statistiques incluent des données relatives à des indicateurs de sécurité clés tels que le nombre de compartiments à usage général accessibles au public ou partagés avec d'autres Comptes AWS. Le tableau de bord affiche également des groupes de données de résultats agrégées pour votre compte, par exemple les noms de 1 à 5 compartiments contenant le plus grand nombre de résultats au cours des sept jours précédents. Vous pouvez effectuer une analyse détaillée de chaque statistique pour consulter ses données justificatives. Pour interroger les statistiques par programmation, utilisez le GetBucketStatisticsfonctionnement de l'API Amazon Macie.

Pour une analyse et une évaluation plus approfondies, Macie fournit des informations et des statistiques détaillées pour les différents compartiments S3 de votre inventaire. Cela inclut le détail des paramètres d'accès public et de chiffrement de chaque compartiment, ainsi que la taille et le

nombre d'objets que Macie peut analyser pour détecter les données sensibles contenues dans le compartiment. L'inventaire indique également si vous avez configuré des tâches de découverte de données sensibles ou si vous avez automatisé la découverte de données sensibles pour analyser les objets d'un compartiment. Si c'est le cas, cela indique quand cette analyse a été effectuée pour la dernière fois. Vous pouvez parcourir, trier et filtrer l'inventaire à l'aide de la console Amazon Macie ou de l'DescribeBucketsAPI Amazon Macie.

Si vous êtes l'administrateur Macie d'une organisation, vous pouvez accéder aux statistiques et aux autres données relatives aux compartiments S3 que possèdent vos comptes membres. Vous pouvez également accéder aux résultats des politiques que Macie génère pour les compartiments et inspecter les compartiments pour détecter la présence de données sensibles. Cela signifie que vous pouvez utiliser Macie pour évaluer et surveiller le niveau de sécurité global du parc de données Amazon S3 de votre entreprise. Pour plus d'informations, voir Gestion de plusieurs comptes .

Rubriques

Comment Amazon Macie surveille la sécurité des données Amazon S3

Lorsque vous activez Amazon Macie pour votre compte Compte AWS, Macie crée actuellement un rôle lié au service AWS Identity and Access Management (IAM) pour votre compte. Région AWS La politique d'autorisation pour ce rôle permet à Macie d'appeler d'autres personnes Services AWS et de surveiller AWS les ressources en votre nom. En utilisant ce rôle, Macie génère et gère un inventaire complet de vos compartiments à usage général Amazon Simple Storage Service (Amazon S3) dans la région. Macie surveille et évalue également les compartiments à des fins de sécurité et de contrôle d'accès.

Si vous êtes l'administrateur Macie d'une organisation, l'inventaire inclut des données statistiques et autres sur les compartiments S3 pour votre compte et les comptes des membres de votre organisation. Grâce à ces données, vous pouvez utiliser Macie pour surveiller et évaluer le niveau de sécurité de votre entreprise dans l'ensemble de votre parc de données Amazon S3. Pour plus d'informations, consultez Gestion de plusieurs comptes .

Rubriques

Composants clés

Amazon Macie utilise une combinaison de fonctionnalités et de techniques pour fournir et gérer les données d'inventaire relatives à vos compartiments S3 à usage général, ainsi que pour surveiller et évaluer les compartiments à des fins de sécurité et de contrôle d'accès.

Collecte de métadonnées et calcul de statistiques

Pour générer et gérer les métadonnées et les statistiques de votre inventaire de compartiments, Macie récupère les métadonnées des compartiments et des objets directement depuis Amazon S3. Pour chaque compartiment, les métadonnées incluent :

- Informations générales sur le bucket, telles que le nom du bucket, le nom Amazon Resource Name (ARN), la date de création, les paramètres de chiffrement, les balises et l' Compte AWS ID de compte du propriétaire du bucket.
- Paramètres d'autorisations au niveau du compte qui s'appliquent au compartiment, tels que les paramètres de blocage de l'accès public pour le compte.
- Paramètres d'autorisations au niveau du compartiment, tels que les paramètres de blocage de l'accès public pour le compartiment et les paramètres dérivés d'une politique de compartiment ou d'une liste de contrôle d'accès (ACL).
- Paramètres d'accès et de réplication partagés pour le compartiment, notamment si les données du compartiment sont répliquées ou partagées avec des Comptes AWS personnes ne faisant pas partie de votre organisation.
- Nombre d'objets et paramètres des objets du compartiment, tels que le nombre d'objets dans le compartiment et la répartition du nombre d'objets par type de chiffrement, type de fichier et classe de stockage.

Macie vous fournit ces informations directement. Macie utilise également ces informations pour calculer des statistiques et fournir des évaluations sur la sécurité et la confidentialité de votre inventaire global et des compartiments individuels de votre inventaire. Par exemple, vous pouvez trouver la taille totale du stockage et le nombre de compartiments dans votre inventaire, la taille

totale du stockage et le nombre d'objets contenus dans ces compartiments, ainsi que la taille totale du stockage et le nombre d'objets que Macie peut analyser pour détecter les données sensibles dans les compartiments.

Par défaut, les métadonnées et les statistiques incluent les données relatives à toutes les parties de l'objet qui existent en raison de chargements partitionnés incomplets. Si vous actualisez manuellement les métadonnées d'un objet pour un bucket spécifique, Macie recalcule les statistiques du bucket et de votre inventaire global, et exclut les données relatives aux parties de l'objet des valeurs recalculées. La prochaine fois que Macie récupérera les métadonnées des compartiments et des objets sur Amazon S3 dans le cadre du cycle d'actualisation quotidien, Macie mettra à jour vos données d'inventaire et inclura à nouveau les données relatives aux parties de l'objet. Pour plus d'informations sur le moment où Macie récupère les métadonnées des compartiments et des objets, consultez. Actualisations de données

Il est important de noter que Macie ne peut pas analyser des parties d'objets pour détecter des données sensibles. Amazon S3 doit d'abord terminer l'assemblage des pièces en un ou plusieurs objets pour que Macie puisse les analyser. Pour plus d'informations sur les chargements partitionnés et les parties d'objets, notamment sur la façon de supprimer automatiquement des parties conformément aux règles du cycle de vie, consultez la section Chargement et copie d'objets à l'aide du téléchargement partitionné dans le guide de l'utilisateur d'Amazon Simple Storage Service. Pour identifier les buckets contenant des parties d'objets, vous pouvez vous référer aux métriques de chargement partitionné incomplètes dans Amazon S3 Storage Lens. Pour plus d'informations, consultez la section Évaluation de votre activité et de votre utilisation du stockage dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Surveillance de la sécurité et de la confidentialité des compartiments

Pour garantir l'exactitude des données au niveau du compartiment dans votre inventaire, Macie surveille et analyse certains AWS CloudTrailévénements susceptibles de se produire pour les données Amazon S3. Si un événement pertinent se produit, Macie met à jour les données d'inventaire appropriées.

Par exemple, si vous activez les paramètres de blocage de l'accès public pour un bucket, Macie met à jour toutes les données relatives aux paramètres d'accès public du bucket. De même, si vous ajoutez ou mettez à jour la politique de compartiment pour un compartiment, Macie analyse la politique et met à jour les données pertinentes de votre inventaire.

Macie surveille et analyse les données relatives aux CloudTrail événements suivants :

- événements au niveau du compte — et DeletePublicAccessBlock PutPublicAccessBlock

- Événements au niveau du bucket :CreateBucket, DeleteAccountPublicAccessBlock, DeleteBucket,DeleteBucketEncryption, DeleteBucketPolicy, DeleteBucketPublicAccessBlock,DeleteBucketReplication, DeleteBucketTagging, PutAccountPublicAccessBlock,,PutBucketAcl, PutBucketEncryption, PutBucketPolicy, PutBucketPublicAccessBlock PutBucketReplication, et PutBucketTagging PutBucketVersioning

Vous ne pouvez pas activer la surveillance pour CloudTrail des événements supplémentaires ou désactiver la surveillance pour aucun des événements précédents. Pour obtenir des informations détaillées sur les opérations correspondantes pour les événements précédents, consultez le manuel Amazon Simple Storage Service API Reference.

> **Tip**
>
> Pour surveiller les événements au niveau des objets, nous vous recommandons d'utiliser la fonctionnalité de protection Amazon S3 d'Amazon. GuardDuty Cette fonctionnalité surveille les événements liés aux données Amazon S3 au niveau des objets et les analyse pour détecter toute activité malveillante ou suspecte. Pour plus d'informations, consultez la section Protection d'Amazon S3 sur Amazon GuardDuty dans le guide de GuardDuty l'utilisateur Amazon.

Évaluation de la sécurité des compartiments et du contrôle d'accès

Pour évaluer la sécurité et le contrôle d'accès au niveau du compartiment, Macie utilise un raisonnement automatique basé sur la logique pour analyser les politiques basées sur les ressources qui s'appliquent à un compartiment. Macie analyse également les paramètres d'autorisation au niveau du compte et du compartiment qui s'appliquent à un compartiment. Cette analyse prend en compte les politiques de compartiment, les ACL au niveau du compartiment et les paramètres de blocage de l'accès public pour le compte et le compartiment.

Pour les politiques basées sur les ressources, Macie utilise Zelkova. Zelkova est un moteur de raisonnement automatisé qui traduit les politiques AWS Identity and Access Management (IAM) en déclarations logiques et exécute une suite de résolveurs logiques spécialisés et à usage général (théories du modulo de satisfaisabilité) pour résoudre le problème de décision. Macie applique Zelkova à plusieurs reprises à une politique avec des requêtes de plus en plus spécifiques pour caractériser les catégories de comportements autorisées par la politique. Pour en savoir plus sur la nature des solveurs utilisés par Zelkova, consultez la section Satisfiability Modulo Theories.

> **Important**
>
> Pour effectuer les tâches précédentes pour un bucket, celui-ci doit être un bucket S3 à usage général. Macie ne surveille ni n'analyse les compartiments de répertoire S3.
> De plus, Macie doit être autorisé à accéder au bucket. Si les paramètres d'autorisation d'un bucket empêchent Macie de récupérer les métadonnées du bucket ou des objets du bucket, Macie ne peut fournir qu'un sous-ensemble d'informations sur le bucket, telles que le nom et la date de création du bucket. Macie ne peut effectuer aucune tâche supplémentaire pour le bucket. Pour plus d'informations, consultez Autoriser Macie à accéder aux compartiments et aux objets S3.

Actualisations de données

Lorsque vous activez Amazon Macie pour votre compte Compte AWS, Macie extrait les métadonnées de vos buckets et objets à usage général S3 directement depuis Amazon S3. Macie récupère ensuite automatiquement les métadonnées des compartiments et des objets directement depuis Amazon S3, dans le cadre d'un cycle d'actualisation quotidien.

Macie récupère également les métadonnées des compartiments directement depuis Amazon S3 lorsque l'une des situations suivantes se produit :

- Vous actualisez vos données d'inventaire en choisissant refresh () sur la console Amazon Macie. Vous pouvez actualiser les données toutes les cinq minutes.
- Vous soumettez une DescribeBucketsdemande à l'API Amazon Macie par programmation et vous n'en avez pas soumis au cours des cinq DescribeBuckets minutes précédentes.
- Macie détecte un AWS CloudTrail événement pertinent.

Macie peut également récupérer les dernières métadonnées d'objets pour un compartiment spécifique si vous choisissez d'actualiser manuellement ces données. Cela peut être utile si vous avez récemment créé un bucket ou si vous avez apporté des modifications importantes aux objets d'un bucket au cours des dernières 24 heures. Pour actualiser manuellement les métadonnées d'un objet pour un compartiment, choisissez refresh () dans la section Statistiques des objets du panneau des détails du compartiment sur la page des

compartiments S3 de la console. Cette fonctionnalité est disponible pour les seaux contenant 30 000 objets ou moins.

Chaque fois que Macie récupère les métadonnées d'un bucket ou d'un objet, Macie met automatiquement à jour toutes les données pertinentes de votre inventaire. Si Macie détecte des différences qui affectent la sécurité ou la confidentialité d'un bucket, Macie commence immédiatement à évaluer et à analyser les modifications. Lorsque l'analyse est terminée, Macie met à jour les données pertinentes de votre inventaire. Si des différences réduisent la sécurité ou la confidentialité d'un bucket, Macie établit également les conclusions de politique appropriées que vous pouvez examiner et corriger si nécessaire.

Pour déterminer à quel moment Macie a récemment récupéré les métadonnées du bucket ou de l'objet pour votre compte, vous pouvez vous référer au champ Dernière mise à jour de la console. Ce champ apparaît sur le tableau de bord récapitulatif, sur la page des compartiments S3 et dans le panneau des détails du compartiment sur la page des compartiments S3. (Si vous utilisez l'API Amazon Macie pour interroger les données d'inventaire, le `lastUpdated` champ fournit ces informations.) Si vous êtes l'administrateur Macie d'une organisation, le champ Dernière mise à jour indique la date et l'heure les plus anciennes auxquelles Macie a récupéré les données d'un compte de votre organisation.

Dans de rares cas, dans certaines conditions, la latence et d'autres problèmes peuvent empêcher Macie de récupérer les métadonnées des compartiments et des objets. Ils peuvent également retarder les notifications que Macie reçoit concernant les modifications apportées à votre inventaire de compartiments ou les paramètres et politiques d'autorisation pour les compartiments individuels. Par exemple, des problèmes de livraison liés à CloudTrail des événements peuvent entraîner des retards. Dans ce cas, Macie analyse les données nouvelles et mises à jour lors de la prochaine actualisation quotidienne, soit dans les 24 heures.

Considérations supplémentaires

Lorsque vous utilisez Amazon Macie pour surveiller et évaluer le niveau de sécurité de vos données Amazon S3, gardez à l'esprit les points suivants :

- Les données d'inventaire ne s'appliquent actuellement Région AWS qu'aux compartiments S3 à usage général. Pour accéder aux données de régions supplémentaires, activez et utilisez Macie dans chaque région supplémentaire.
- Si vous êtes l'administrateur Macie d'une organisation, vous pouvez accéder aux données d'inventaire d'un compte membre uniquement si Macie est activé pour ce compte dans la région actuelle.

- Si les paramètres d'autorisation d'un bucket empêchent Macie de récupérer des informations sur le bucket ou les objets du bucket, Macie ne peut pas évaluer et surveiller la sécurité et la confidentialité des données du bucket ou fournir des informations détaillées sur le bucket.

  Pour vous aider à identifier un compartiment dans lequel c'est le cas, Macie effectue les opérations suivantes :

  - Dans l'inventaire de votre compartiment, Macie affiche une icône d'avertissement (⚠) pour le compartiment. Pour les détails du bucket, Macie affiche uniquement un sous-ensemble de champs et de données : l'ID de compte du Compte AWS propriétaire du bucket ; le nom du bucket, Amazon Resource Name (ARN), la date de création et la région ; et la date et l'heure auxquelles Macie a récemment récupéré les métadonnées du bucket et de l'objet pour le bucket dans le cadre du cycle d'actualisation quotidien. Si vous utilisez l'API Amazon Macie pour interroger les données d'inventaire, Macie fournit un code d'erreur et un message pour le compartiment, et la valeur de la plupart des propriétés du compartiment est nulle.
  - Dans le tableau de bord récapitulatif, le bucket a la valeur Inconnu pour les statistiques d'accès public, de chiffrement et de partage. (Si vous utilisez l'API Amazon Macie pour interroger les statistiques, le bucket a une valeur de `unknown` pour ces statistiques.) En outre, Macie exclut le bucket lorsqu'il calcule les données pour les statistiques relatives au stockage et aux objets.

  Pour étudier le problème, consultez la politique du compartiment et les paramètres d'autorisation dans Amazon S3. Par exemple, le compartiment peut avoir une politique de compartiment restrictive. Pour plus d'informations, consultez Autoriser Macie à accéder aux compartiments et aux objets S3.

- Les données relatives à l'accès et aux autorisations sont limitées aux paramètres du compte et du bucket. Il ne reflète pas les paramètres au niveau de l'objet qui déterminent l'accès à des objets spécifiques dans un compartiment. Par exemple, si l'accès public est activé pour un objet spécifique dans un bucket, Macie n'indique pas que le bucket ou les objets du bucket sont accessibles au public.

  Pour surveiller les opérations au niveau des objets et identifier les risques de sécurité potentiels, nous vous recommandons d'utiliser la fonctionnalité de protection Amazon S3 d'Amazon. GuardDuty Cette fonctionnalité surveille les événements liés aux données Amazon S3 au niveau des objets et les analyse pour détecter toute activité malveillante ou suspecte. Pour plus d'informations, consultez la section Protection d'Amazon S3 sur Amazon GuardDuty dans le guide de GuardDuty l'utilisateur Amazon.

- Si vous actualisez manuellement les métadonnées d'un objet pour un compartiment spécifique, Macie signale temporairement Unknown pour les statistiques de chiffrement qui s'appliquent aux objets. La prochaine fois que Macie procédera à l'actualisation quotidienne des données (dans les 24 heures), Macie réévaluera les métadonnées de chiffrement des objets et rapportera à nouveau des données quantitatives pour les statistiques.
- Si vous actualisez manuellement les métadonnées d'un objet pour un bucket spécifique, Macie exclut temporairement les données de toutes les parties d'objet contenues dans le bucket en raison de chargements partitionnés incomplets. La prochaine fois que Macie procédera à l'actualisation quotidienne des données (dans les 24 heures), Macie recalcule le nombre et les valeurs de taille de stockage pour les objets du bucket et inclut les données relatives aux pièces dans ces calculs.
- Dans de rares cas, Macie peut ne pas être en mesure de déterminer si un bucket est accessible au public ou partagé, ou si les nouveaux objets doivent être chiffrés côté serveur. Par exemple, un problème temporaire peut empêcher Macie de récupérer et d'analyser les données requises. Il se peut également que Macie ne soit pas en mesure de déterminer complètement si une ou plusieurs déclarations de politique accordent l'accès à une entité externe. Dans ces cas, Macie indique « Inconnu » pour les statistiques et les champs pertinents de l'inventaire. Pour étudier ces cas, consultez la politique du compartiment et les paramètres d'autorisation dans Amazon S3.

Notez également que Macie génère des conclusions relatives aux politiques uniquement si la sécurité ou la confidentialité d'un bucket sont réduites une fois que vous avez activé Macie pour votre compte. Par exemple, si vous désactivez les paramètres de blocage de l'accès public pour un bucket après avoir activé Macie, Macie génère une recherche BlockPublicAccessDisabledPolicy:IAMuser/S3 pour le bucket. Toutefois, si les paramètres de blocage de l'accès public ont été désactivés pour un bucket lorsque vous avez activé Macie et qu'ils continuent de l'être, Macie ne génère pas de recherche BlockPublicAccessDisabledPolicy:IAMuser/S3 pour le bucket.

En outre, lorsque Macie évalue la sécurité et la confidentialité d'un bucket, il n'examine pas les journaux d'accès ni n'analyse les utilisateurs, les rôles et les autres configurations pertinentes pour les comptes. Au lieu de cela, Macie analyse et rapporte les données relatives aux paramètres clés qui indiquent les risques de sécurité potentiels. Par exemple, si une constatation de politique indique qu'un compartiment est accessible au public, cela ne signifie pas nécessairement qu'une entité externe a accédé au compartiment. De même, si une politique indique qu'un bucket est partagé avec une personne Compte AWS extérieure à votre organisation, Macie n'essaie pas de déterminer si cet accès est intentionnel et sûr. Ces résultats indiquent plutôt qu'une entité externe peut potentiellement accéder aux données du compartiment, ce qui peut constituer un risque de sécurité involontaire.

Évaluation de votre niveau de sécurité Amazon S3 avec Amazon Macie

Pour évaluer le niveau de sécurité global de vos données Amazon Simple Storage Service (Amazon S3) et déterminer les mesures à prendre, vous pouvez utiliser le tableau de bord récapitulatif de la console Amazon Macie.

Le tableau de bord récapitulatif fournit un aperçu des statistiques agrégées relatives à vos données Amazon S3 actuelles Région AWS. Les statistiques incluent des données relatives à des indicateurs de sécurité clés tels que le nombre de compartiments à usage général accessibles au public ou partagés avec d'autres Comptes AWS personnes. Le tableau de bord affiche également des groupes de données de résultats agrégées pour votre compte, par exemple les types de résultats ayant enregistré le plus grand nombre d'occurrences au cours des sept jours précédents. Si vous êtes l'administrateur Macie d'une organisation, le tableau de bord fournit des statistiques et des données agrégées pour tous les comptes de votre organisation. Vous pouvez éventuellement filtrer les données par compte.

Pour effectuer une analyse plus approfondie, vous pouvez explorer et consulter les données de support relatives à des éléments individuels sur le tableau de bord. Vous pouvez également consulter et analyser l'inventaire de votre compartiment S3 à l'aide de la console Amazon Macie, ou interroger et analyser les données d'inventaire par programmation en utilisant l'API Amazon DescribeBucketsMacie.

Rubriques

Afficher le tableau de bord récapitulatif

Sur la console Amazon Macie, le tableau de bord récapitulatif fournit un aperçu des statistiques agrégées et des données de résultats pour vos données Amazon S3 actuelles. Région AWS Si vous préférez interroger les statistiques par programmation, vous pouvez utiliser le GetBucketStatisticsfonctionnement de l'API Amazon Macie.

Pour afficher le tableau de bord récapitulatif

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Résumé. Macie affiche le tableau de bord récapitulatif.
3. Pour savoir à quel moment Macie a récemment récupéré les métadonnées de bucket ou d'objet d'Amazon S3 pour votre compte, reportez-vous au champ Dernière mise à jour en haut du tableau de bord. Pour plus d'informations, consultez Actualisations de données.
4. Pour accéder aux données justificatives d'un élément du tableau de bord et passer en revue les données correspondantes, sélectionnez l'élément en question.

Si vous êtes l'administrateur Macie d'une organisation, le tableau de bord affiche des statistiques et des données agrégées pour votre compte et les comptes des membres de votre organisation. Pour filtrer le tableau de bord et afficher les données uniquement pour un compte en particulier, entrez l'identifiant du compte dans le champ Compte situé au-dessus du tableau de bord.

Comprendre les composants du tableau de bord récapitulatif

Dans le tableau de bord récapitulatif, les statistiques et les données sont organisées en plusieurs sections. En haut du tableau de bord, vous trouverez des statistiques agrégées qui indiquent la quantité de données que vous stockez dans Amazon S3 et la quantité de données qu'Amazon Macie peut analyser pour détecter les données sensibles. Vous pouvez également consulter le champ Dernière mise à jour pour déterminer à quel moment Macie a récemment récupéré les métadonnées de bucket ou d'objet d'Amazon S3 pour votre compte. Des sections supplémentaires fournissent des statistiques et des données récentes qui peuvent vous aider à évaluer la sécurité, la confidentialité et la sensibilité de vos données Amazon S3 à l'heure actuelle Région AWS.

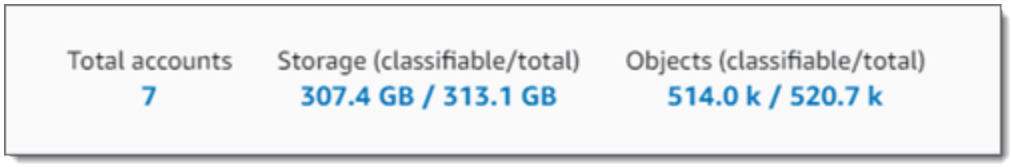
Les statistiques et les données sont organisées dans les sections suivantes :

Stockage et découverte de données sensibles | Problèmes de découverte et de couverture automatisés | Sécurité des données | Principaux compartiments S3 | Principaux types de détection | Conclusions relatives aux politiques

Lorsque vous passez en revue chaque section, choisissez éventuellement un élément à explorer vers le bas et examinez les données justificatives. Notez également que le tableau de bord n'inclut pas les données relatives aux compartiments de répertoire S3, mais uniquement les compartiments à usage général. Macie ne surveille ni n'analyse les compartiments de répertoires.

Stockage et découverte de données sensibles

Les statistiques en haut du tableau de bord indiquent la quantité de données que vous stockez dans Amazon S3 et la quantité de données que Macie peut analyser pour détecter les données sensibles. Par exemple :



Dans cette section :

- Nombre total de comptes — Ce champ apparaît si vous êtes l'administrateur Macie d'une organisation ou si vous possédez un compte Macie autonome. Il indique le nombre total de Comptes AWS ces propres compartiments dans votre inventaire de compartiments. Si vous êtes administrateur Macie, il s'agit du nombre total de comptes Macie que vous gérez pour votre organisation. Si vous avez un compte Macie autonome, cette valeur est 1.

  Nombre total de compartiments S3 : ce champ apparaît si votre compte Macie est membre d'une organisation. Il indique le nombre total de seaux à usage général présents dans votre inventaire, y compris les seaux qui ne contiennent aucun objet.
- Stockage : ces indicateurs fournissent des informations sur la taille de stockage des objets de votre inventaire de compartiments :
  - Classifiable : taille de stockage totale de tous les objets que Macie peut analyser dans les compartiments.
  - Total : taille de stockage totale de tous les objets contenus dans les compartiments, y compris les objets que Macie ne peut pas analyser.

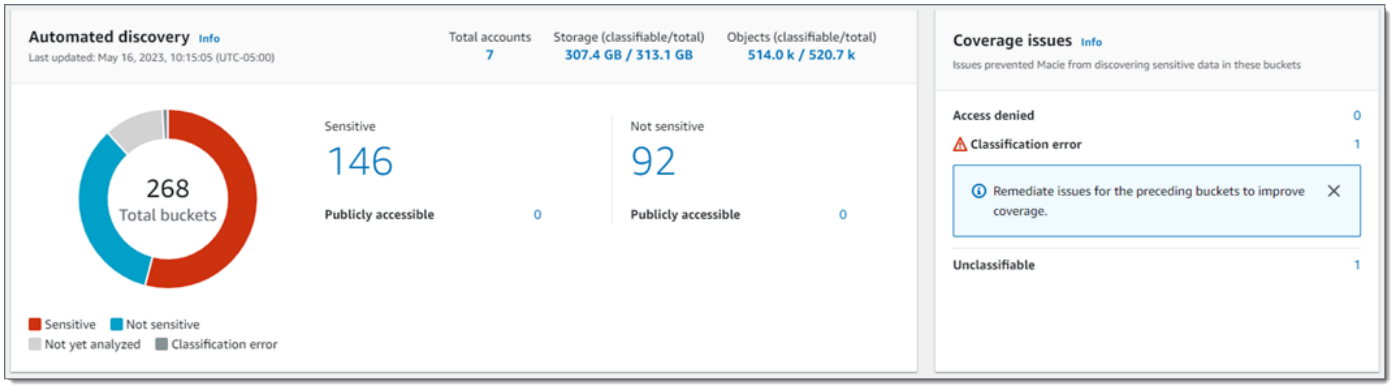
  Si l'un des objets est un fichier compressé, ces valeurs ne reflètent pas la taille réelle de ces fichiers après leur décompression. Si le versionnement est activé pour l'un des compartiments, ces valeurs sont basées sur la taille de stockage de la dernière version de chaque objet contenu dans ces compartiments.
- Objets : ces statistiques fournissent des informations sur le nombre d'objets contenus dans votre inventaire de compartiments :
  - Classifiable : nombre total d'objets que Macie peut analyser dans les compartiments.
  - Total : nombre total d'objets contenus dans les compartiments, y compris les objets que Macie ne peut pas analyser.

Dans les statistiques précédentes, les données et les objets sont classifiables s'ils utilisent une classe de stockage Amazon S3 prise en charge et s'ils possèdent une extension de nom de fichier pour un format de fichier ou de stockage pris en charge. Vous pouvez détecter des données sensibles dans les objets à l'aide de Macie. Pour plus d'informations, consultez Classes et formats de stockage pris en charge.

Notez que les statistiques relatives au stockage et aux objets n'incluent pas les données relatives aux objets contenus dans des compartiments auxquels Macie n'est pas autorisé à accéder. Par exemple, des objets placés dans des compartiments soumis à des politiques de compartiment restrictives. Pour identifier les compartiments dans lesquels c'est le cas, vous pouvez consulter votre inventaire de compartiments à l'aide du tableau des compartiments S3. Si l'icône d'avertissement (⚠) apparaît à côté du nom d'un bucket, Macie n'est pas autorisé à accéder au bucket.

Problèmes de découverte et de couverture automatisés

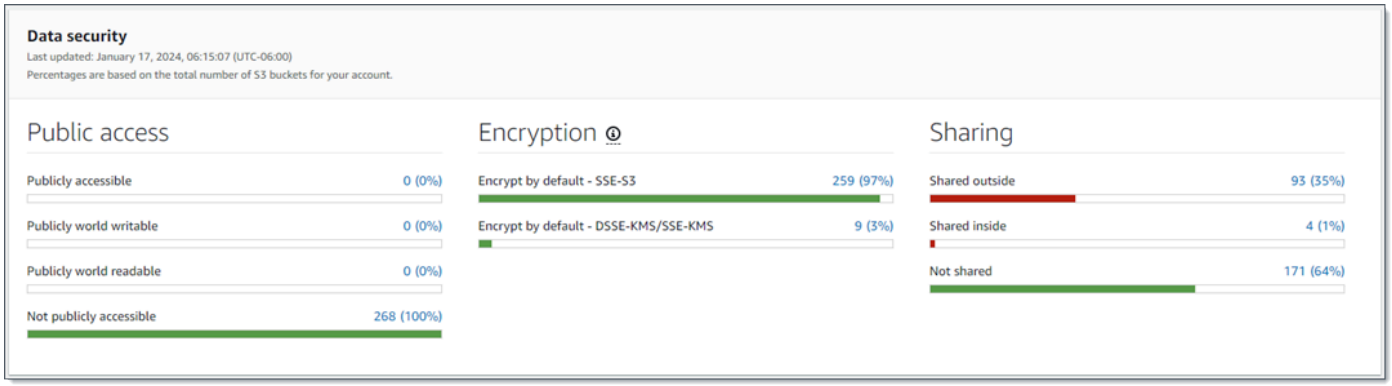
Si la découverte automatique des données sensibles est activée, ces sections apparaissent sur le tableau de bord. Les statistiques présentées dans ces sections présentent l'état et les résultats des activités automatisées de découverte de données sensibles que Macie a effectuées jusqu'à présent pour vos données Amazon S3. Par exemple :



Pour plus de détails sur ces statistiques, consultezExamen des statistiques agrégées de sensibilité des données sur le tableau de bord récapitulatif.

Sécurité des données

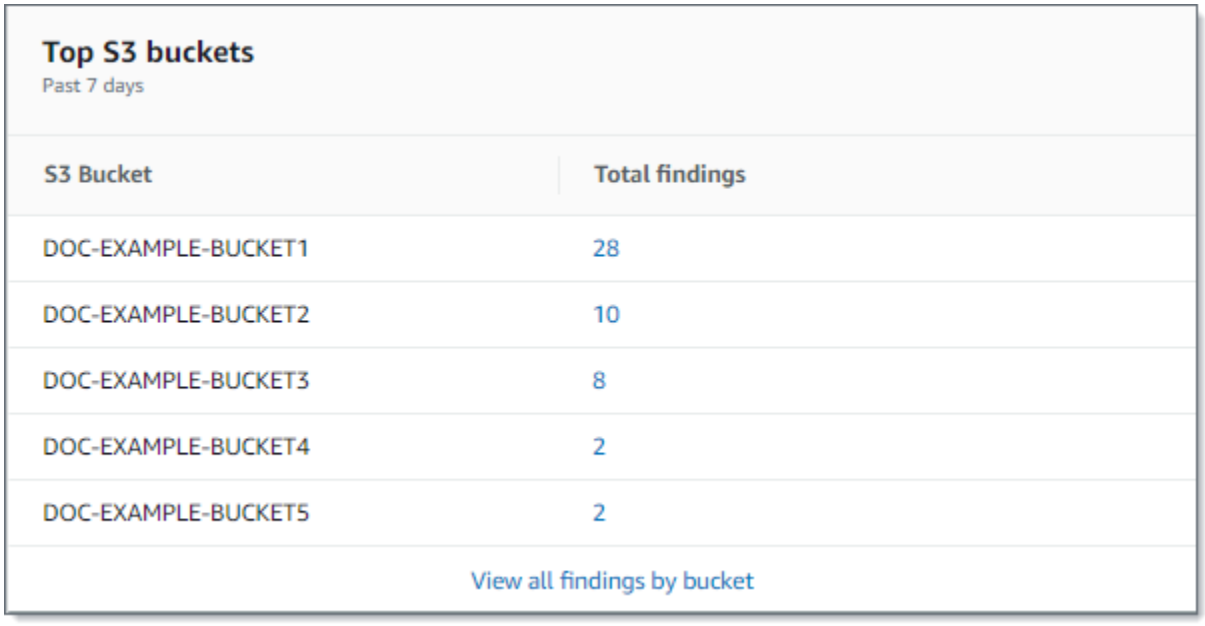
Cette section fournit des statistiques qui indiquent les risques potentiels liés à la sécurité et à la confidentialité de vos données Amazon S3. Par exemple :



Pour plus de détails sur ces statistiques, consultezComprendre les statistiques de sécurité des données sur le tableau de bord récapitulatif.

Les meilleurs seaux S3

Cette section répertorie les compartiments S3 qui ont généré le plus grand nombre de résultats, tous types confondus, au cours des sept jours précédents, pour un maximum de cinq compartiments. Il indique également le nombre de résultats créés par Macie pour chaque compartiment. Par exemple :

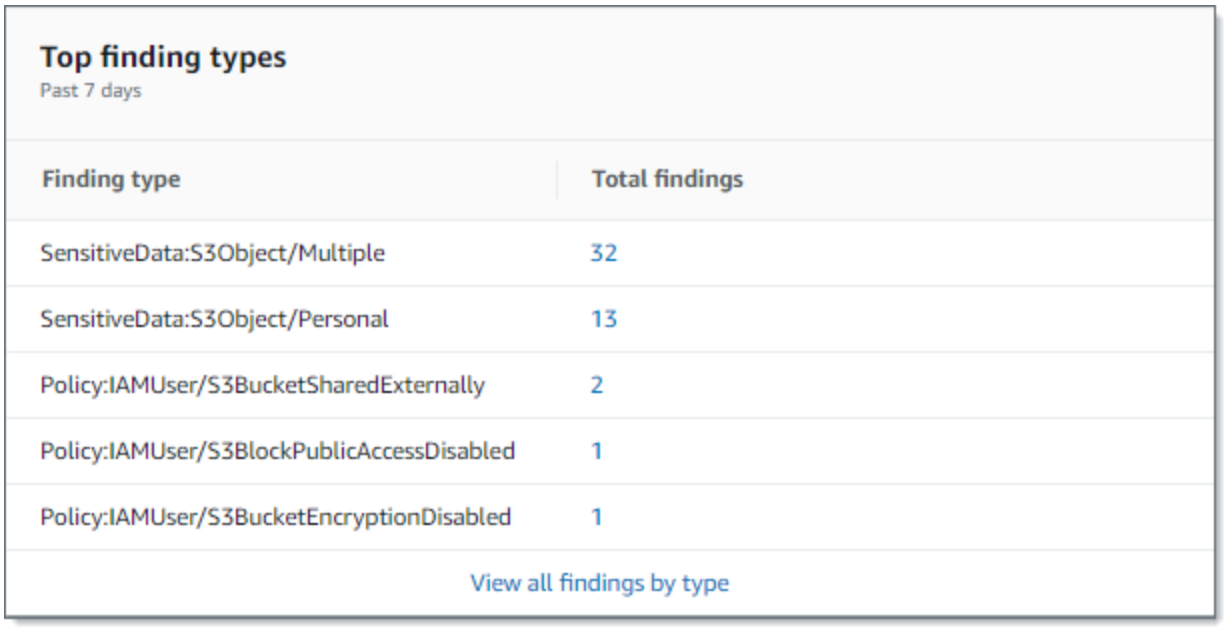


Pour afficher et éventuellement explorer tous les résultats d'un bucket au cours des sept jours précédents, choisissez la valeur dans le champ Total des résultats. Pour afficher tous les résultats actuels de tous vos compartiments, regroupés par compartiment, choisissez Afficher tous les résultats par compartiment.

Cette section est vide si Macie n'a créé aucun résultat au cours des sept jours précédents. Ou toutes les découvertes créées au cours des sept jours précédents ont été supprimées par une règle de suppression.

Principaux types de recherche

Cette section répertorie les types de constatations qui ont enregistré le plus grand nombre d'occurrences au cours des sept jours précédents, pour un maximum de cinq types de constatations. Il indique également le nombre de résultats créés par Macie pour chaque type. Par exemple :



Pour afficher et éventuellement approfondir tous les résultats d'un type particulier des sept jours précédents, choisissez la valeur dans le champ Total des résultats. Pour afficher tous les résultats actuels, regroupés par type de recherche, choisissez Afficher tous les résultats par type.

Cette section est vide si Macie n'a créé aucun résultat au cours des sept jours précédents. Ou toutes les découvertes créées au cours des sept jours précédents ont été supprimées par une règle de suppression.

Résultats politiques

Cette section répertorie les conclusions politiques que Macie a créées ou mises à jour récemment, pour un maximum de dix conclusions. Par exemple :

Pour afficher les détails d'un résultat en particulier, choisissez-le.

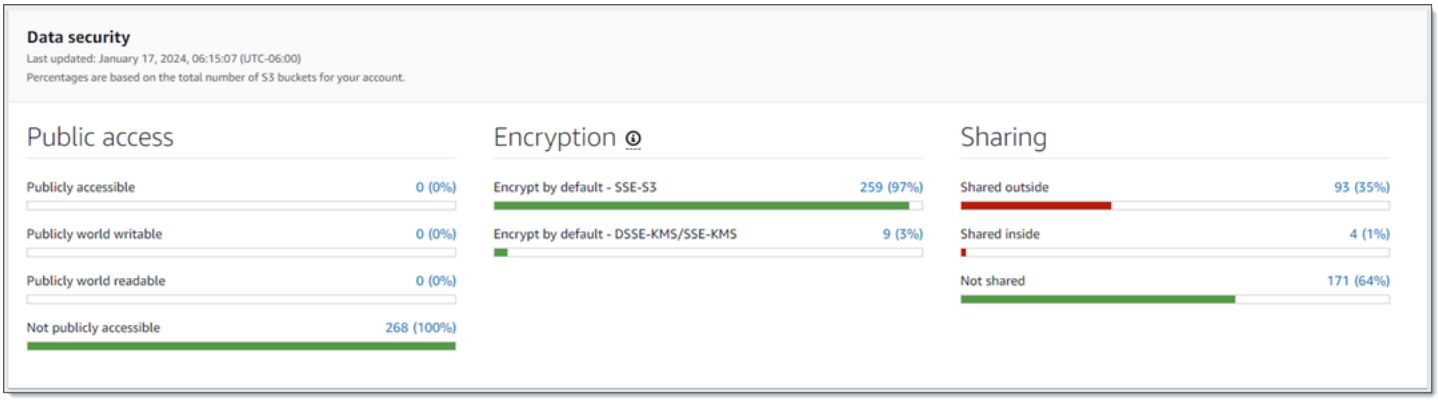
Cette section est vide si Macie n'a pas créé ou mis à jour de conclusions relatives aux politiques au cours des sept jours précédents. Ou toutes les conclusions relatives aux politiques créées ou mises à jour au cours des sept jours précédents ont été supprimées par une règle de suppression.

Comprendre les statistiques de sécurité des données sur le tableau de bord récapitulatif

La section Sécurité des données du tableau de bord récapitulatif fournit des statistiques qui peuvent vous aider à identifier et à étudier les risques potentiels liés à la sécurité et à la confidentialité de vos données Amazon S3 dans le contexte actuel Région AWS. Par exemple, vous pouvez utiliser ces données pour identifier les compartiments à usage général accessibles au public ou partagés avec d'autres Comptes AWS.

Si votre compte Macie appartient à une organisation, les statistiques de stockage et de découverte de données sensibles présentées en haut de cette section indiquent la quantité de données que vous stockez dans Amazon S3 et la quantité de données que Macie peut analyser pour détecter les données sensibles.

Pour tout type de compte Macie, les statistiques supplémentaires sont organisées en trois zones, comme le montre l'image suivante.



Au fur et à mesure que vous passez en revue chaque domaine, choisissez éventuellement un élément à explorer vers le bas et examinez les données justificatives. Notez également que les statistiques n'incluent pas les données relatives aux compartiments de répertoire S3, mais uniquement les compartiments à usage général. Macie ne surveille ni n'analyse les compartiments de répertoires.

Les statistiques individuelles dans chaque domaine sont les suivantes.

Accès public

Ces statistiques indiquent combien de compartiments S3 sont ou ne sont pas accessibles au public :

- Accessible au public : nombre et pourcentage de compartiments qui permettent au grand public d'avoir un accès en lecture ou en écriture au compartiment.
- Accessible au public dans le monde entier : nombre et pourcentage de compartiments qui permettent au grand public d'avoir un accès en écriture au compartiment.
- Lisible par le public : nombre et pourcentage de compartiments qui permettent au grand public d'avoir un accès en lecture au compartiment.
- Non accessible au public : nombre et pourcentage de compartiments qui n'autorisent pas le grand public à accéder au compartiment en lecture ou en écriture.

Pour calculer chaque pourcentage, Macie divise le nombre de compartiments applicables par le nombre total de compartiments dans votre inventaire de compartiments.

Pour déterminer les valeurs de cette section, Macie analyse une combinaison de paramètres au niveau du compte et du compartiment pour chaque compartiment : les paramètres de blocage de l'accès public pour le compte ; les paramètres de blocage de l'accès public pour le compartiment ; la politique du compartiment ; et la liste de contrôle d'accès (ACL) pour le compartiment. Pour plus

d'informations sur ces paramètres, consultez Gestion des identités et des accès dans Amazon S3 et Blocage de l'accès public à votre espace de stockage Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Dans certains cas, la section Accès public affiche également des valeurs pour Inconnu. Si ces valeurs apparaissent, Macie n'a pas été en mesure d'évaluer les paramètres d'accès public pour le nombre et le pourcentage de compartiments spécifiés. Par exemple, un problème temporaire ou les paramètres d'autorisation des compartiments ont empêché Macie de récupérer les données requises. Ou Macie n'a pas été en mesure de déterminer complètement si une ou plusieurs déclarations de politique autorisaient une entité externe à accéder aux compartiments.

Chiffrement

Ces statistiques indiquent le nombre de compartiments S3 configurés pour appliquer certains types de chiffrement côté serveur aux objets ajoutés aux compartiments :

- Chiffrer par défaut — SSE-S3 — Nombre et pourcentage de compartiments dont les paramètres de chiffrement par défaut sont configurés pour chiffrer de nouveaux objets avec une clé gérée par Amazon S3. Pour ces compartiments, les nouveaux objets sont chiffrés automatiquement à l'aide du chiffrement SSE-S3.
- Chiffrement par défaut — DSSE-KMS/SSE-KMS — Nombre et pourcentage de compartiments dont les paramètres de chiffrement par défaut sont configurés pour chiffrer les nouveaux objets à l'aide d'une clé gérée par le client ou d'une AWS KMS key clé gérée par le client. Clé gérée par AWS Pour ces compartiments, les nouveaux objets sont chiffrés automatiquement à l'aide du chiffrement DSSE-KMS ou SSE-KMS.

Pour calculer chaque pourcentage, Macie divise le nombre de compartiments applicables par le nombre total de compartiments dans votre inventaire de compartiments.

Pour déterminer les valeurs de cette section, Macie analyse les paramètres de chiffrement par défaut pour chaque compartiment. À compter du 5 janvier 2023, Amazon S3 applique automatiquement le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de chiffrement de base pour les objets ajoutés aux compartiments. Vous pouvez éventuellement configurer les paramètres de chiffrement par défaut d'un compartiment pour utiliser à la place le chiffrement côté serveur avec une AWS KMS clé (SSE-KMS) ou le chiffrement double couche côté serveur avec une clé (DSSE-KMS). AWS KMS Pour plus d'informations sur les paramètres et options de chiffrement par défaut, consultez la section Définition du comportement de chiffrement côté serveur par défaut pour les compartiments S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Dans certains cas, la section Chiffrement affiche également des valeurs pour Inconnu. Si ces valeurs apparaissent, Macie n'a pas été en mesure d'évaluer les paramètres de chiffrement par défaut pour le nombre et le pourcentage de compartiments spécifiés. Par exemple, un problème temporaire ou les paramètres d'autorisation des compartiments ont empêché Macie de récupérer les données requises.

Partage

Ces statistiques indiquent le nombre de compartiments S3 partagés ou non avec d'autres entités Comptes AWS, qu'il s'agisse d'identités d'accès à l' CloudFront origine (OAI) ou de contrôles CloudFront d'accès à l'origine (OAC) d'Amazon :

- Partagé en externe : nombre et pourcentage de buckets partagés avec un ou plusieurs des organismes suivants ou une combinaison des éléments suivants : un CloudFront OAI, un CloudFront OAC ou un compte qui n'appartient pas à la même organisation.
- Partagé en interne : nombre et pourcentage de buckets partagés avec un ou plusieurs comptes de la même organisation. Ces compartiments ne sont pas partagés avec les OAI ou les CloudFront OAC.
- Non partagé : nombre et pourcentage de compartiments qui ne sont pas partagés avec d'autres comptes, CloudFront OAI ou CloudFront OAC.

Pour calculer chaque pourcentage, Macie divise le nombre de compartiments applicables par le nombre total de compartiments dans votre inventaire de compartiments.

Pour déterminer si les buckets sont partagés avec d'autres Comptes AWS, Macie analyse la politique de bucket et l'ACL pour chaque bucket. En outre, une organisation est définie comme un ensemble de comptes Macie gérés de manière centralisée en tant que groupe de comptes connexes via AWS Organizations ou sur invitation de Macie. Pour plus d'informations sur les options d'Amazon S3 pour le partage de compartiments, consultez la section Gestion des identités et des accès dans Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

> **Note**
>
> Dans certains cas, Macie peut signaler à tort qu'un bucket est partagé avec un utilisateur Compte AWS n'appartenant pas à la même organisation. Cela peut se produire si Macie n'est pas en mesure d'évaluer pleinement la relation entre l'`Principal`élément de la politique d'un compartiment et certaines clés de contexte de condition AWS globales ou certaines clés de condition Amazon S3 présentes dans l'`Condition`élément de la politique. Les clés de condition

applicables sont les suivantes : `aws:PrincipalAccount` `aws:PrincipalArn` `aws:PrincipalOrgIDaws:PrincipalOrgPaths`,`aws:PrincipalTag`,`aws:PrincipalType`, `ets3:DataAccessPointArn`.
Pour déterminer si c'est le cas pour les compartiments individuels, choisissez la statistique externe partagée sur le tableau de bord. Dans le tableau qui apparaît, notez le nom de chaque compartiment. Utilisez ensuite Amazon S3 pour examiner la politique de chaque compartiment et déterminer si les paramètres d'accès partagé sont intentionnels et sûrs.

Pour déterminer si les compartiments sont partagés avec des OAI ou des CloudFront OAC, Macie analyse la politique de compartiment pour chaque compartiment. Un CloudFront OAI ou un OAC permet aux utilisateurs d'accéder aux objets d'un bucket via une ou plusieurs distributions spécifiées CloudFront. Pour plus d'informations sur les CloudFront OAI et les OAC, consultez Restreindre l'accès à une origine Amazon S3 dans le manuel Amazon CloudFront Developer Guide.

Dans certains cas, la section Partage affiche également des valeurs pour Inconnu. Si ces valeurs apparaissent, Macie n'a pas été en mesure de déterminer si le nombre et le pourcentage de buckets spécifiés sont partagés avec d'autres comptes, CloudFront OAI ou OAC. CloudFront Par exemple, un problème temporaire ou les paramètres d'autorisation des compartiments ont empêché Macie de récupérer les données requises. Ou Macie n'a pas été en mesure d'évaluer pleinement les politiques ou les ACL des compartiments.

Analyse de votre posture de sécurité Amazon S3 avec Amazon Macie

Pour vous aider à effectuer une analyse approfondie et à évaluer le niveau de sécurité de vos données Amazon Simple Storage Service (Amazon S3), Amazon Macie tient un inventaire complet de vos compartiments S3 à usage général dans Région AWS chaque endroit où vous utilisez Macie. Pour savoir comment Macie gère cet inventaire pour vous, consultezComment Macie surveille la sécurité des données Amazon S3. Si vous êtes l'administrateur Macie d'une organisation, l'inventaire inclut les données relatives aux compartiments S3 que possèdent vos comptes membres.

En utilisant cet inventaire, vous pouvez consulter votre parc de données Amazon S3 et examiner les détails et les statistiques des principaux paramètres et mesures de sécurité qui s'appliquent aux compartiments S3 individuels. Par exemple, vous pouvez accéder au détail des paramètres d'accès public et de chiffrement de chaque compartiment, ainsi qu'à la taille et au nombre d'objets que

Macie peut analyser pour détecter les données sensibles dans chaque compartiment. Vous pouvez également déterminer si vous avez configuré des tâches de découverte de données sensibles ou si vous avez automatisé la découverte de données sensibles pour analyser les objets d'un compartiment. Si c'est le cas, les données de votre inventaire indiquent à quel moment cette analyse a été effectuée pour la dernière fois. Si la découverte automatique des données sensibles est activée, vous pouvez également utiliser l'inventaire pour examiner les résultats des activités de découverte automatique de données sensibles que Macie a effectuées jusqu'à présent pour vos données Amazon S3. Pour plus d'informations, consultez Découverte de données sensibles.

Vous pouvez parcourir et filtrer les données d'inventaire en utilisant la page des compartiments S3 sur la console Amazon Macie. Vous pouvez également accéder à vos données d'inventaire par programmation en utilisant l'DescribeBucketsAPI Amazon Macie.

Rubriques

- Révision de l'inventaire de votre compartiment S3 avec Amazon Macie
- Filtrer l'inventaire de votre compartiment S3 avec Amazon Macie

Révision de l'inventaire de votre compartiment S3 avec Amazon Macie

Sur la console Amazon Macie, la page des compartiments S3 fournit des informations détaillées sur la sécurité et la confidentialité de vos données Amazon Simple Storage Service (Amazon S3) actuelles. Région AWS Cette page vous permet de consulter et d'analyser un inventaire complet de vos compartiments S3 à usage général dans la région, ainsi que de consulter des informations et des statistiques détaillées pour chaque compartiment. Si vous êtes l'administrateur Macie d'une organisation, votre inventaire inclut les détails et les statistiques des compartiments S3 que possèdent vos comptes membres.

La page des compartiments S3 indique également à quel moment Macie a récemment récupéré les métadonnées de compartiment ou d'objet d'Amazon S3 pour votre compte. Vous trouverez ces informations dans le champ Dernière mise à jour en haut de la page. Si vous êtes l'administrateur Macie d'une organisation, ce champ indique la date et l'heure les plus anciennes auxquelles Macie a récupéré les données d'un compte dans votre organisation. Pour plus d'informations, consultez Actualisations de données.

Notez que les données d'inventaire et les statistiques n'incluent pas les données relatives aux compartiments de répertoire S3, mais uniquement les compartiments à usage général. Macie ne surveille ni n'analyse les compartiments de répertoires. En outre, la plupart des données d'inventaire sont limitées aux compartiments auxquels Macie est autorisée à accéder pour votre compte. Si

les paramètres d'autorisation d'un bucket empêchent Macie de récupérer des informations sur le bucket ou les objets du bucket, Macie ne peut fournir qu'un sous-ensemble d'informations sur le bucket. Si tel est le cas pour un compartiment en particulier, Macie affiche une icône d'avertissement (⚠) et un message pour le compartiment dans votre inventaire de compartiments. Pour les détails du bucket, Macie affiche uniquement un sous-ensemble de champs et de données : l'ID de compte du propriétaire du Compte AWS bucket ; le nom du bucket, Amazon Resource Name (ARN), la date de création et la région ; et la date à laquelle Macie a récemment récupéré les métadonnées du bucket et de l'objet pour le bucket dans le cadre du cycle d'actualisation quotidien. Pour étudier le problème, consultez la politique du compartiment et les paramètres d'autorisation dans Amazon S3. Par exemple, le compartiment peut avoir une politique de compartiment restrictive. Pour plus d'informations, consultez Autoriser Macie à accéder aux compartiments et aux objets S3.

Si vous préférez accéder à vos données d'inventaire et les interroger par programmation, vous pouvez utiliser l'DescribeBucketsAPI Amazon Macie.

Rubriques

- Révision de l'inventaire de votre compartiment S3
- Examiner les détails des compartiments S3

Révision de l'inventaire de votre compartiment S3

La page des compartiments S3 de la console Amazon Macie fournit des informations sur vos compartiments S3 à usage général actuels. Région AWS Sur cette page, un tableau affiche des informations récapitulatives pour chaque compartiment de votre inventaire. Pour personnaliser votre affichage, vous pouvez trier et filtrer le tableau. Si vous choisissez un bucket dans le tableau, le panneau de détails affiche des informations supplémentaires sur le bucket. Cela inclut des détails et des statistiques sur les paramètres et les mesures qui fournissent un aperçu de la sécurité et de la confidentialité des données du bucket. Vous pouvez éventuellement exporter les données du tableau vers un fichier de valeurs séparées par des virgules (CSV).

Si la découverte automatique des données sensibles est activée, vous avez également la possibilité de consulter votre inventaire à l'aide d'une carte thermique interactive. La carte fournit une représentation visuelle de la sensibilité des données dans l'ensemble de votre parc de données Amazon S3. Il capture les résultats des activités automatisées de découverte de données sensibles effectuées par Macie jusqu'à présent. Pour en savoir plus sur cette carte, voirVisualisation de la sensibilité des données avec la carte des compartiments S3.

Pour consulter l'inventaire de votre compartiment S3

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez S3 buckets (Compartiments S3).
   La page des compartiments S3 affiche l'inventaire de vos compartiments.
   Si la page affiche une carte interactive de votre inventaire, choisissez table
   ()
   en haut de la page. Macie affiche ensuite le nombre de seaux dans votre inventaire et un tableau des seaux.

   Si la découverte automatique des données sensibles est activée, la vue par défaut n'affiche pas les données des buckets actuellement exclus de la découverte automatique. Pour afficher ces données, choisissez X dans le jeton de filtre Is monitoring by automated discovery situé sous le filtre.
3. En haut de la page, choisissez éventuellement refresh
   ()
   pour récupérer les dernières métadonnées du bucket depuis Amazon S3.

   Si l'icône d'information
   ()
   apparaît à côté d'un nom de bucket, nous vous recommandons de le faire. Cette icône indique qu'un bucket a été créé au cours des dernières 24 heures, probablement après que Macie ait récupéré pour la dernière fois les métadonnées du bucket et de l'objet sur Amazon S3 dans le cadre du cycle d'actualisation quotidien.
4. Sur la page des compartiments S3, utilisez le tableau pour consulter un sous-ensemble d'informations concernant chaque compartiment de votre inventaire :

   - Sensibilité : score de sensibilité actuel du compartiment. Cette colonne apparaît uniquement si la découverte automatique des données sensibles est activée. Pour plus d'informations sur la plage de scores de sensibilité définie par Macie, consultezNotation de sensibilité pour les compartiments S3.
   - Bucket : nom du bucket.
   - Compte : ID de compte du Compte AWS propriétaire du bucket.
   - Objets classifiables : nombre total d'objets que Macie peut analyser pour détecter les données sensibles contenues dans le compartiment.

- Taille classifiable : taille de stockage totale de tous les objets que Macie peut analyser pour détecter les données sensibles dans le compartiment.

  Notez que cette valeur ne reflète pas la taille réelle des objets compressés après leur décompression. En outre, si le versionnement est activé pour le compartiment, cette valeur est basée sur la taille de stockage de la dernière version de chaque objet du compartiment.
- Surveillé par tâche : si des tâches de découverte de données sensibles sont configurées pour analyser régulièrement les objets du compartiment sur une base quotidienne, hebdomadaire ou mensuelle.

  Si la valeur de ce champ est Oui, le compartiment est explicitement inclus dans une tâche périodique ou le compartiment a répondu aux critères d'une tâche périodique au cours des dernières 24 heures. En outre, le statut d'au moins un de ces emplois n'est pas annulé. Macie met à jour ces données quotidiennement.
- Dernière exécution de la tâche : si des tâches ponctuelles ou périodiques de découverte de données sensibles sont configurées pour analyser les objets du compartiment, ce champ indique la date et l'heure les plus récentes auxquelles l'une de ces tâches a commencé à s'exécuter. Dans le cas contraire, un tiret (—) apparaît dans ce champ.

Dans les données précédentes, les objets sont classifiables s'ils utilisent une classe de stockage Amazon S3 prise en charge et s'ils possèdent une extension de nom de fichier pour un format de fichier ou de stockage pris en charge. Vous pouvez détecter des données sensibles dans les objets à l'aide de Macie. Pour plus d'informations, consultez Classes et formats de stockage pris en charge.

5. Pour analyser votre inventaire à l'aide du tableau, effectuez l'une des opérations suivantes :

   - Pour trier le tableau en fonction d'un champ spécifique, choisissez l'en-tête de colonne du champ. Pour modifier l'ordre de tri, choisissez à nouveau l'en-tête de colonne.
   - Pour filtrer le tableau et n'afficher que les compartiments contenant une valeur spécifique pour un champ, placez votre curseur dans la zone de filtre, puis ajoutez une condition de filtre pour le champ. Pour affiner davantage les résultats, ajoutez des conditions de filtre pour des champs supplémentaires. Pour plus d'informations, consultez Filtrer l'inventaire de votre compartiment S3.
6. Pour consulter les détails et les statistiques d'un bucket en particulier, choisissez le nom du bucket dans le tableau, puis consultez le panneau des détails.

> **Tip**
>
> Vous pouvez pivoter et effectuer une exploration vers le bas sur de nombreux champs du panneau des détails du compartiment. Pour afficher les compartiments ayant la même valeur pour un champ, choisissez
>
> 
>
> dans le champ. Pour afficher les compartiments contenant d'autres valeurs pour un champ, choisissez
>
> 
>
> dans le champ.

7. Pour exporter les données du tableau vers un fichier CSV, cochez la case correspondant à chaque ligne que vous souhaitez exporter ou cochez la case dans l'en-tête de la colonne de sélection pour sélectionner toutes les lignes. Choisissez ensuite Exporter au format CSV en haut de la page. Vous pouvez exporter jusqu'à 50 000 lignes depuis le tableau.

Examiner les détails des compartiments S3

Sur la console Amazon Macie, vous pouvez utiliser le panneau de détails de la page des compartiments S3 pour consulter les statistiques et d'autres informations concernant chaque compartiment à usage général de votre inventaire de compartiments S3. Cela inclut des détails et des statistiques sur les paramètres et les mesures qui fournissent un aperçu de la sécurité et de la confidentialité des données d'un bucket.

Par exemple, vous pouvez consulter le détail des paramètres d'accès public d'un compartiment S3 et déterminer si un compartiment est configuré pour répliquer des objets ou s'il est partagé avec d'autres. Comptes AWS Vous pouvez également déterminer si des tâches de découverte de données sensibles sont configurées pour inspecter le compartiment à la recherche de données sensibles. Si tel est le cas, vous pouvez accéder aux détails de la tâche exécutée le plus récemment et éventuellement afficher les résultats produits par la tâche.

Si la découverte automatique des données sensibles est activée, vous pouvez également utiliser le panneau de détails pour consulter les statistiques de découverte de données sensibles et d'autres informations sur les compartiments S3 individuels. Le panneau capture les résultats des activités automatisées de découverte de données sensibles que Macie a effectuées jusqu'à présent pour un bucket. Pour en savoir plus sur ces détails, consultezExamen des détails relatifs à la sensibilité des données pour les compartiments S3 individuels.

Pour consulter les détails d'un compartiment S3

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez S3 buckets (Compartiments S3). La page des compartiments S3 affiche l'inventaire de vos compartiments.

   Si la découverte automatique des données sensibles est activée, la vue par défaut n'affiche pas les données des buckets actuellement exclus de la découverte automatique. Pour afficher ces données, choisissez X dans le jeton de filtre Is monitoring by automated discovery situé sous le filtre.
3. En haut de la page, choisissez éventuellement refresh
   ()
   pour récupérer les dernières métadonnées du bucket depuis Amazon S3.
4. Choisissez le compartiment dont vous souhaitez consulter les informations. Le panneau de détails affiche des statistiques et d'autres informations sur le bucket.

Dans le panneau de détails, les statistiques et les informations sont organisées dans les sections principales suivantes :

Vue d'ensemble | Statistiques des objets | Chiffrement côté serveur | Découverte de données sensibles | Accès public | Réplication | Tags

Lorsque vous passez en revue les informations de chaque section, vous pouvez éventuellement pivoter et parcourir certains champs vers le bas. Pour afficher les compartiments ayant la même valeur pour un champ, choisissez

dans le champ. Pour afficher les compartiments contenant d'autres valeurs pour un champ, choisissez

dans le champ.

Présentation

Cette section fournit des informations générales sur le bucket, telles que le nom du bucket, la date de création du bucket et l'ID de compte du Compte AWS propriétaire du bucket. Il convient de noter que le champ Dernière mise à jour indique la date à laquelle Macie a récemment récupéré les métadonnées du bucket ou des objets du bucket sur Amazon S3.

Le champ Accès partagé indique si le compartiment est partagé avec une autre personne Compte AWS, une identité CloudFront d'accès d'origine Amazon (OAI) ou un contrôle CloudFront d'accès d'origine (OAC) :

- Externe : le bucket est partagé avec un ou plusieurs des éléments suivants ou une combinaison des éléments suivants : un CloudFront OAI, un CloudFront OAC ou un compte externe à votre organisation (n'en faisant pas partie).
- Interne : le bucket est partagé avec un ou plusieurs comptes internes à (une partie de) votre organisation. Il n'est pas partagé avec un CloudFront OAI ou un OAC.
- Non partagé : le bucket n'est pas partagé avec un autre compte, un CloudFront OAI ou un CloudFront OAC.
- Inconnu : Macie n'a pas pu évaluer les paramètres d'accès partagé pour le compartiment.

Pour déterminer si un bucket est partagé avec un autre Compte AWS, Macie analyse la politique du bucket et la liste de contrôle d'accès (ACL) du bucket. L'analyse est limitée aux paramètres au niveau du compartiment. Il ne reflète aucun paramètre au niveau de l'objet pour le partage d'objets spécifiques dans le compartiment. En outre, une organisation est définie comme un ensemble de comptes Macie gérés de manière centralisée en tant que groupe de comptes connexes via AWS Organizations ou sur invitation de Macie. Pour en savoir plus sur les options d'Amazon S3 pour le partage de compartiments, consultez la section Gestion des identités et des accès dans Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

> **Note**
>
> Dans certains cas, Macie peut indiquer à tort qu'un bucket est partagé avec un Compte AWS utilisateur externe (ne faisant pas partie de) votre organisation. Cela peut se produire si Macie n'est pas en mesure d'évaluer pleinement la relation entre l'`Principal`élément de la politique du compartiment et certaines clés de contexte de condition AWS globales ou les clés de condition Amazon S3 présentes dans l'`Condition`élément de la politique. Les clés de condition applicables sont les suivantes : `aws:PrincipalAccount` `aws:PrincipalArn` `aws:PrincipalOrgID`aws:PrincipalOrgPaths,aws:PrincipalTag,aws:PrincipalType,aws:PrincipalArn`s3:DataAccessPointArn`. Nous vous recommandons de consulter la politique du bucket afin de déterminer si cet accès est prévu et sûr.

Pour déterminer si un bucket est partagé avec un CloudFront OAI ou un OAC, Macie analyse la politique de bucket applicable au bucket. Un CloudFront OAI ou un OAC permet aux utilisateurs d'accéder aux objets d'un bucket via une ou plusieurs distributions spécifiées CloudFront . Pour en savoir plus sur les CloudFront OAI et les OAC, consultez Restreindre l'accès à une origine Amazon S3 dans le manuel Amazon CloudFront Developer Guide.

La section Vue d'ensemble inclut également le champ Dernière exécution de découverte automatique. Ce champ indique à quel moment Macie a récemment analysé les objets du compartiment lors de la découverte automatique de données sensibles. Si cette analyse n'a pas eu lieu, un tiret (—) apparaît dans ce champ.

Statistiques sur les objets

Cette section fournit des informations sur les objets du compartiment, en commençant par le nombre total d'objets contenus dans le compartiment (nombre total), la taille de stockage totale de tous ces objets (taille de stockage totale) et la taille de stockage totale de tous les objets qui sont des fichiers compressés (.gz, .gzip ou .zip) (taille compressée totale). Les statistiques supplémentaires présentées dans cette section peuvent vous aider à évaluer la quantité de données que Macie peut analyser pour détecter les données sensibles présentes dans le compartiment.

Si vous avez récemment créé le bucket ou apporté des modifications importantes aux objets du bucket au cours des dernières 24 heures, choisissez éventuellement refresh () pour récupérer les dernières métadonnées des objets du bucket. Macie affiche l'icône d'information () pour vous aider à déterminer si tel est le cas. L'option d'actualisation est disponible si un bucket contient 30 000 objets ou moins.

Lorsque vous examinez les statistiques présentées dans cette section, gardez les points suivants à l'esprit :

- Si le versionnement est activé pour le compartiment, les valeurs de taille sont basées sur la taille de stockage de la dernière version de chaque objet du compartiment.
- Si le bucket stocke des objets compressés, les valeurs de taille ne reflètent pas la taille réelle de ces objets après leur décompression.
- Si vous actualisez les métadonnées d'un objet pour un bucket, Macie signale temporairement Unknown pour les statistiques de chiffrement qui s'appliquent aux objets. Macie réévaluera et mettra à jour les données de ces statistiques lors de la prochaine actualisation quotidienne des métadonnées des compartiments et des objets, qui aura lieu dans les 24 heures.

- Par défaut, le nombre d'objets et les valeurs de taille incluent les données relatives à toutes les parties d'objets contenues dans le bucket à la suite de chargements partitionnés incomplets. Si vous actualisez les métadonnées d'un objet pour un bucket, Macie exclut les données relatives aux parties de l'objet des valeurs recalculées. Lorsque Macie effectue la prochaine actualisation quotidienne des métadonnées du bucket et de l'objet (dans les 24 heures), Macie recalcule et met à jour les valeurs de ces statistiques et inclut à nouveau les données relatives aux parties de l'objet dans les valeurs.

  Notez que Macie ne peut pas analyser les parties de l'objet pour détecter des données sensibles. Amazon S3 doit d'abord terminer l'assemblage des pièces en un ou plusieurs objets pour que Macie puisse les analyser. Pour plus d'informations sur les chargements partitionnés et les parties d'objets, notamment sur la façon de supprimer automatiquement des parties conformément aux règles du cycle de vie, consultez la section Chargement et copie d'objets à l'aide du téléchargement partitionné dans le guide de l'utilisateur d'Amazon Simple Storage Service. Pour identifier les buckets contenant des parties d'objets, vous pouvez vous référer aux métriques de chargement partitionné incomplètes dans Amazon S3 Storage Lens. Pour plus d'informations, consultez la section Évaluation de votre activité et de votre utilisation du stockage dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Les statistiques des objets sont organisées comme suit.

Objets classifiables

Cette section indique le nombre total d'objets que Macie peut analyser pour détecter des données sensibles et la taille de stockage totale de ces objets. Ces objets utilisent une classe de stockage Amazon S3 prise en charge et possèdent une extension de nom de fichier correspondant à un format de fichier ou de stockage pris en charge. Vous pouvez détecter des données sensibles dans les objets à l'aide de Macie. Pour plus d'informations, consultez Classes et formats de stockage pris en charge.

Objets inclassables

Cette section indique le nombre total d'objets que Macie ne peut pas analyser pour détecter des données sensibles et la taille de stockage totale de ces objets. Ces objets n'utilisent pas de classe de stockage Amazon S3 prise en charge ou ne possèdent pas d'extension de nom de fichier pour un format de fichier ou de stockage pris en charge.

Objets inclassables : classe de stockage

Cette section fournit une ventilation du nombre et de la taille de stockage des objets que Macie ne peut pas analyser car ils n'utilisent pas de classe de stockage Amazon S3 prise en charge.

Objets inclassables : type de fichier

Cette section fournit une ventilation du nombre et de la taille de stockage des objets que Macie ne peut pas analyser car ils ne possèdent pas d'extension de nom de fichier pour un format de fichier ou de stockage pris en charge.

Objets par type de chiffrement

Cette section fournit une ventilation du nombre d'objets qui utilisent chaque type de chiffrement pris en charge par Amazon S3 :

- Fourni par le client : nombre d'objets chiffrés à l'aide d'une clé fournie par le client. Ces objets utilisent le chiffrement SSE-C.
- AWS KMS géré : nombre d'objets chiffrés à l'aide d'une AWS KMS key clé gérée par le client Clé gérée par AWS ou d'une clé gérée par le client. Ces objets utilisent le chiffrement DSSE-KMS ou SSE-KMS.
- géré par Amazon S3 : nombre d'objets chiffrés à l'aide d'une clé gérée par Amazon S3. Ces objets utilisent le chiffrement SSE-S3.
- Pas de chiffrement : nombre d'objets qui ne sont pas chiffrés ou qui utilisent le chiffrement côté client. (Si un objet est chiffré à l'aide du chiffrement côté client, Macie ne peut pas accéder aux données de chiffrement de l'objet et les rapporter.)
- Inconnu : nombre d'objets pour lesquels Macie ne dispose pas de métadonnées de chiffrement actuelles. Cela se produit généralement si vous avez récemment choisi d'actualiser manuellement les métadonnées des objets du compartiment. Macie mettra à jour les statistiques de chiffrement lors de la prochaine actualisation quotidienne des métadonnées des compartiments et des objets, dans les 24 heures.

Pour plus d'informations sur chaque type de chiffrement pris en charge, consultez la section Protection des données par le chiffrement dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Chiffrement côté serveur

Cette section fournit un aperçu des paramètres de chiffrement côté serveur pour le compartiment.

Le champ Chiffrement requis par la politique du bucket indique si la politique du bucket exige le chiffrement des objets côté serveur lorsque des objets sont ajoutés au bucket :

- Non : le bucket n'a pas de politique de bucket ou la politique du bucket n'exige pas le chiffrement des nouveaux objets côté serveur. S'il existe une politique de compartiment, elle n'exige pas que les PutObjectdemandes incluent un en-tête de chiffrement côté serveur valide.
- Oui — La politique du bucket exige le chiffrement des nouveaux objets côté serveur. PutObjectles demandes relatives au compartiment doivent inclure un en-tête de chiffrement côté serveur valide. Sinon, Amazon S3 refuse la demande.
- Inconnu : Macie n'a pas été en mesure d'évaluer la politique du compartiment pour déterminer s'il nécessite le chiffrement des nouveaux objets côté serveur.

Pour cette évaluation, les en-têtes de chiffrement côté serveur valides sont les suivants : `x-amz-server-side-encryption` avec une valeur de `AES256` ou`aws:kms`, et `x-amz-server-side-encryption-customer-algorithm` avec une valeur de. `AES256` Pour plus d'informations sur l'utilisation de politiques de compartiment pour exiger le chiffrement côté serveur des nouveaux objets, consultez la section Protection des données par le chiffrement côté serveur dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Le champ Chiffrement par défaut indique l'algorithme de chiffrement côté serveur que le bucket est configuré pour appliquer par défaut aux objets ajoutés au bucket :

- AES256 — Les paramètres de chiffrement par défaut du compartiment sont configurés pour chiffrer les nouveaux objets à l'aide d'une clé gérée par Amazon S3. Les nouveaux objets sont chiffrés automatiquement à l'aide du chiffrement SSE-S3.
- aws:kms — Les paramètres de chiffrement par défaut du compartiment sont configurés pour chiffrer les nouveaux objets à l'aide d'une AWS KMS key clé gérée par le client Clé gérée par AWS ou d'une clé gérée par le client. Les nouveaux objets sont chiffrés automatiquement à l'aide du chiffrement SSE-KMS. Le AWS KMS keychamp indique le nom de ressource Amazon (ARN) ou l'identifiant unique (ID de clé) de la clé utilisée.
- aws:kms:dsse — Les paramètres de chiffrement par défaut du compartiment sont configurés pour chiffrer les nouveaux objets à l'aide d'une clé gérée par le client ou d'une clé gérée par AWS KMS key le client. Clé gérée par AWS Les nouveaux objets sont chiffrés automatiquement à l'aide du chiffrement DSSE-KMS. Le AWS KMS keychamp indique l'ARN ou l'ID de clé de la clé utilisée.
- Aucun : les paramètres de chiffrement par défaut du compartiment ne spécifient pas le comportement de chiffrement côté serveur pour les nouveaux objets.

À compter du 5 janvier 2023, Amazon S3 applique automatiquement le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de chiffrement de base pour les objets ajoutés aux compartiments. Vous pouvez éventuellement configurer les paramètres de chiffrement par défaut d'un compartiment pour utiliser à la place le chiffrement côté serveur avec une AWS KMS clé (SSE-KMS) ou le chiffrement double couche côté serveur avec une clé (DSSE-KMS). AWS KMS Pour plus d'informations sur les paramètres et options de chiffrement par défaut, consultez la section Définition du comportement de chiffrement côté serveur par défaut pour les compartiments S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Découverte de données sensibles

Cette section indique si les tâches de découverte de données sensibles sont configurées pour analyser régulièrement les objets du compartiment sur une base quotidienne, hebdomadaire ou mensuelle. Si la valeur du champ Surveillance active par tâche est Oui, le compartiment est explicitement inclus dans une tâche périodique ou le compartiment a répondu aux critères d'une tâche périodique au cours des dernières 24 heures. En outre, le statut d'au moins un de ces emplois n'est pas annulé. Macie met à jour ces données quotidiennement.

Si un type de tâche de découverte de données sensibles (tâche périodique ou ponctuelle) est configuré pour inspecter le compartiment, le champ Dernière tâche fournit l'identifiant unique de la tâche qui a récemment commencé à s'exécuter. Le champ Dernière exécution de la tâche indique la date à laquelle cette tâche a commencé à s'exécuter.

> **Tip**
>
> Pour afficher toutes les données sensibles trouvées par la tâche, cliquez sur le lien dans le champ Dernière tâche. Dans le panneau des détails de la tâche qui apparaît, choisissez Afficher les résultats en haut du panneau, puis choisissez Afficher les résultats.

Accès public

Cette section indique si le bucket est accessible au public. Il fournit également une ventilation des différents paramètres au niveau du compte et du bucket qui déterminent si tel est le cas. Le champ Autorisation effective indique le résultat cumulé de ces paramètres :

- Non public : le compartiment n'est pas accessible au public.
- Public : le compartiment est accessible au public.
- Inconnu : Macie n'a pas été en mesure d'évaluer tous les paramètres d'accès public du bucket.

Notez que ces données sont limitées aux paramètres au niveau du compte et du bucket. Il ne reflète pas les paramètres au niveau des objets qui permettent au public d'accéder à des objets spécifiques d'un compartiment.

Pour en savoir plus sur les paramètres Amazon S3 relatifs à la gestion de l'accès public aux compartiments et aux données des compartiments, consultez les sections Gestion des identités et des accès dans Amazon S3 et Blocage de l'accès public à votre espace de stockage Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Réplication

Dans cette section, le champ Répliqué indique si le compartiment est configuré pour répliquer des objets vers d'autres compartiments. Si la valeur de ce champ est Oui, une ou plusieurs règles de réplication sont configurées et activées pour le compartiment. Cette section répertorie également l'ID de compte de chaque propriétaire Compte AWS d'un compartiment de destination.

Le champ Répliqué en externe indique si le bucket est configuré pour répliquer des objets vers des buckets externes (ne faisant pas partie de) votre organisation. Comptes AWS Une organisation est un ensemble de comptes Macie gérés de manière centralisée en tant que groupe de comptes connexes via AWS Organizations ou sur invitation de Macie. Si la valeur de ce champ est Oui, une règle de réplication est configurée et activée pour le compartiment, et la règle est configurée pour répliquer des objets dans un compartiment appartenant à un utilisateur externe Compte AWS.

> **Note**
>
> Dans certaines conditions, Macie peut indiquer à tort qu'un bucket est configuré pour répliquer des objets vers un bucket appartenant à un utilisateur externe. Compte AWS Cela peut se produire si le compartiment de destination a été créé différemment Région AWS au cours des 24 heures précédentes, après que Macie ait récupéré les métadonnées du bucket et de l'objet sur Amazon S3 dans le cadre du cycle d'actualisation quotidien.
> Pour étudier le problème à l'aide de Macie, choisissez refresh
> ()
> pour récupérer les dernières métadonnées du bucket depuis Amazon S3. Passez ensuite en revue la liste des identifiants de compte dans cette section. Pour une analyse plus approfondie, utilisez Amazon S3 pour passer en revue les règles de réplication du compartiment.

Pour en savoir plus sur les options et les paramètres d'Amazon S3 pour la réplication d'objets de compartiment, consultez la section Réplication d'objets dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Balises

Si des balises sont associées au bucket, cette section apparaît dans le panneau et répertorie ces balises. Les balises sont des étiquettes que vous pouvez définir et attribuer à certains types de AWS ressources, notamment les compartiments S3. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative.

Pour en savoir plus sur le balisage des compartiments, consultez la section Utilisation des balises de compartiment S3 pour la répartition des coûts dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Filtrer l'inventaire de votre compartiment S3 avec Amazon Macie

Pour identifier et cibler les compartiments présentant des caractéristiques spécifiques, vous pouvez filtrer votre inventaire de compartiments S3 sur la console Amazon Macie et dans les requêtes que vous soumettez par programmation à l'aide de l'API Amazon Macie. Lorsque vous créez un filtre, vous utilisez des attributs de compartiment spécifiques pour définir des critères permettant d'inclure ou d'exclure des compartiments d'une vue ou des résultats de requête. Un attribut de compartiment est un champ qui stocke des métadonnées spécifiques pour un compartiment.

Dans Macie, un filtre comprend une ou plusieurs conditions. Chaque condition, également appelée critère, comprend trois parties :

- Un champ basé sur un attribut, tel que le nom du compartiment, la clé de balise ou Defined in job.
- Un opérateur, tel que égal ou non égal.
- Une ou plusieurs valeurs. Le type et le nombre de valeurs dépendent du champ et de l'opérateur que vous choisissez.

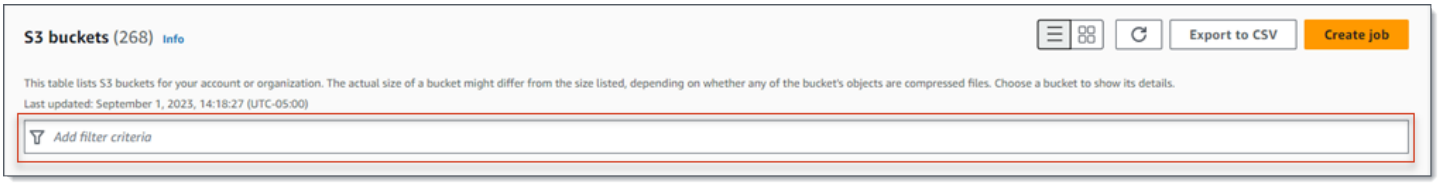
La façon dont vous définissez et appliquez les conditions de filtrage dépend de votre utilisation de la console Amazon Macie ou de l'API Amazon Macie.

Rubriques

- Filtrer votre inventaire sur la console Amazon Macie
- Filtrer votre inventaire par programmation avec l'API Amazon Macie

Filtrer votre inventaire sur la console Amazon Macie

Si vous utilisez la console Amazon Macie pour filtrer l'inventaire de vos compartiments S3, Macie propose des options pour vous aider à choisir les champs, les opérateurs et les valeurs correspondant à des conditions individuelles. Vous pouvez accéder à ces options en utilisant le champ de filtre sur la page des compartiments S3, comme illustré dans l'image suivante.

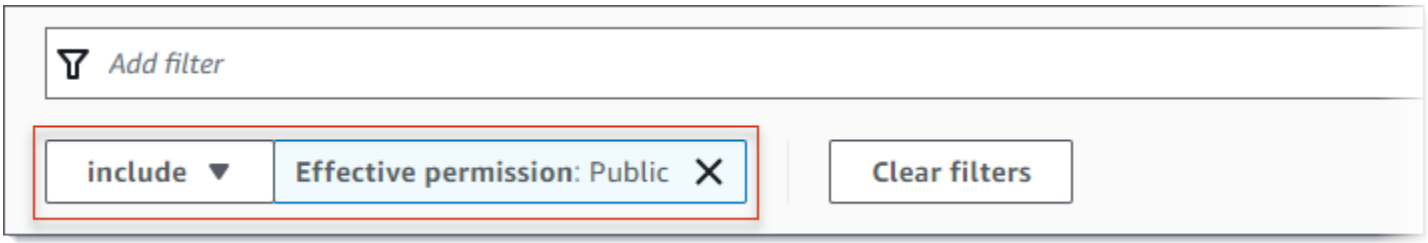


Lorsque vous placez votre curseur dans la zone de filtre, Macie affiche une liste de champs que vous pouvez utiliser dans des conditions de filtrage. Les champs sont organisés par catégorie logique. Par exemple, la catégorie Champs communs inclut les champs qui stockent des informations générales sur un compartiment S3. Les catégories d'accès public incluent des champs qui stockent des données relatives aux différents types de paramètres d'accès public qui peuvent s'appliquer à un bucket. Les champs sont triés par ordre alphabétique au sein de chaque catégorie.

Pour ajouter une condition, commencez par choisir un champ dans la liste. Pour trouver un champ, parcourez la liste complète ou entrez une partie du nom du champ pour affiner la liste des champs.

Selon le champ que vous choisissez, Macie affiche différentes options. Les options reflètent le type et la nature du champ que vous choisissez. Par exemple, si vous choisissez le champ Accès partagé, Macie affiche une liste de valeurs parmi lesquelles choisir. Si vous choisissez le champ Nom du compartiment, Macie affiche une zone de texte dans laquelle vous pouvez saisir le nom d'un compartiment S3. Quel que soit le champ que vous choisissez, Macie vous guide à travers les étapes pour ajouter une condition incluant les paramètres requis pour le champ.

Après avoir ajouté une condition, Macie applique les critères de la condition et affiche la condition dans un jeton de filtre situé sous la boîte de filtre, comme illustré dans l'image suivante.



Dans cet exemple, la condition est configurée pour inclure tous les compartiments accessibles au public et pour exclure tous les autres compartiments. Elle renvoie des compartiments dont la valeur du champ Autorisation effective est égale à Public.

Au fur et à mesure que vous ajoutez des conditions, Macie applique leurs critères et les affiche sous la zone de filtre. Si vous ajoutez plusieurs conditions, Macie utilise la logique AND pour joindre les conditions et évaluer les critères de filtrage. Cela signifie qu'un compartiment S3 correspond aux critères du filtre uniquement s'il répond à toutes les conditions du filtre. Vous pouvez vous référer à tout moment à la zone située sous la boîte de filtre pour déterminer les critères que vous avez appliqués.

Pour filtrer votre inventaire à l'aide de la console

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez S3 buckets (Compartiments S3). La page des compartiments S3 affiche l'inventaire de vos compartiments.

   Si la découverte automatique des données sensibles est activée, la vue par défaut n'affiche pas les données des buckets actuellement exclus de la découverte automatique. Si vous êtes l'administrateur Macie d'une organisation, elle n'affiche pas non plus les données des comptes pour lesquels la découverte automatique est actuellement désactivée. Pour afficher ces données, choisissez X dans le jeton de filtre Is monitoring by automated discovery situé sous le filtre.
3. En haut de la page, choisissez éventuellement refresh
   ()
   pour récupérer les dernières métadonnées du bucket depuis Amazon S3.
4. Placez votre curseur dans la zone de filtre, puis choisissez le champ à utiliser pour la condition.
5. Choisissez ou entrez le type de valeur approprié pour le champ, en tenant compte des conseils suivants.

   Dates, heures et plages horaires

   Pour les dates et les heures, utilisez les champs From et To pour définir une plage horaire inclusive :

   - Pour définir une plage horaire fixe, utilisez les champs From et To pour spécifier la première date et l'heure ainsi que les dernières date et heure de la plage, respectivement.

- Pour définir une plage de temps relative qui commence à une certaine date et heure et se termine à l'heure actuelle, entrez la date et l'heure de début dans les zones De et supprimez tout texte dans les zones À.
- Pour définir une plage de temps relative se terminant à une certaine date et heure, entrez la date et l'heure de fin dans les zones À et supprimez le texte dans les zones De.

Notez que les valeurs temporelles utilisent une notation de 24 heures. Si vous utilisez le sélecteur de dates pour choisir des dates, vous pouvez affiner les valeurs en saisissant du texte directement dans les zones De et À.

Numéros et plages numériques

Pour les valeurs numériques, utilisez les champs From et To pour saisir des nombres entiers qui définissent une plage numérique inclusive :

- Pour définir une plage numérique fixe, utilisez les zones From et To pour spécifier les nombres les plus bas et les plus élevés de la plage, respectivement.
- Pour définir une plage numérique fixe limitée à une valeur spécifique, entrez la valeur dans les champs De et À. Par exemple, pour inclure uniquement les compartiments S3 qui stockent exactement 15 objets, entrez **`15`** dans les champs From et To.
- Pour définir une plage numérique relative commençant à un certain nombre, entrez le nombre dans la zone De et n'entrez aucun texte dans la zone À.
- Pour définir une plage numérique relative qui se termine à un certain nombre, entrez le numéro dans la zone À et ne saisissez aucun texte dans la zone De.

Valeurs de texte (chaîne)

Pour ce type de valeur, entrez une valeur complète et valide pour le champ. Les valeurs distinguent les majuscules et minuscules.

Notez que vous ne pouvez pas utiliser de valeur partielle ou de caractères génériques dans ce type de valeur. La seule exception est le champ du nom du compartiment. Pour ce champ, vous pouvez spécifier un préfixe au lieu d'un nom de compartiment complet. Par exemple, pour rechercher tous les compartiments S3 dont le nom commence par My-S3, entrez la valeur **`my-S3`** de filtre dans le champ Nom du compartiment. Si vous entrez une autre valeur, telle que **`My-s3`** ou**`my*`**, Macie ne retournera pas les seaux.

6. Lorsque vous avez fini d'ajouter une valeur au champ, choisissez Appliquer. Macie applique les critères du filtre et affiche la condition dans un jeton de filtre situé sous la boîte de filtre.
7. Répétez les étapes 4 à 6 pour chaque condition supplémentaire que vous souhaitez ajouter.

8. Pour supprimer une condition, choisissez le X dans le jeton de filtre correspondant à la condition.
9. Pour modifier une condition, supprimez-la en choisissant le X dans le jeton de filtre correspondant à la condition. Répétez ensuite les étapes 4 à 6 pour ajouter une condition avec les paramètres appropriés.

Filtrer votre inventaire par programmation avec l'API Amazon Macie

Pour filtrer l'inventaire de votre compartiment S3 par programmation, spécifiez des critères de filtrage dans les requêtes que vous soumettez à l'aide de DescribeBucketsl'API Amazon Macie. Cette opération renvoie un tableau d'objets. Chaque objet contient des données statistiques et d'autres informations sur un compartiment correspondant aux critères du filtre.

Pour spécifier des critères de filtre dans une requête, incluez une carte des conditions de filtre dans votre demande. Pour chaque condition, spécifiez un champ, un opérateur et une ou plusieurs valeurs pour le champ. Le type et le nombre de valeurs dépendent du champ et de l'opérateur que vous choisissez. Pour plus d'informations sur les champs, les opérateurs et les types de valeurs que vous pouvez utiliser dans une condition, consultez les sources de données Amazon S3 dans le manuel Amazon Macie API Reference.

Les exemples suivants vous montrent comment spécifier des critères de filtre dans les requêtes que vous soumettez à l'aide du AWS Command Line Interface (AWS CLI). Vous pouvez également le faire en utilisant une version actuelle d'un autre outil de ligne de AWS commande ou d'un AWS SDK, ou en envoyant des requêtes HTTPS directement à Macie. Pour plus d'informations sur AWS les outils et les SDK, voir Outils sur AWS lesquels s'appuyer.

Exemples

- Exemple 1 : Rechercher des compartiments par nom de compartiment
- Exemple 2 : trouver des compartiments accessibles au public
- Exemple 3 : Rechercher des compartiments contenant des objets non chiffrés
- Exemple 4 : Rechercher des compartiments qui ne sont pas surveillés par une tâche
- Exemple 5 : trouver des compartiments qui répliquent les données vers des comptes externes
- Exemple 6 : Rechercher des compartiments en fonction de plusieurs critères

Les exemples utilisent la commande describe-buckets. Si un exemple s'exécute correctement, Macie renvoie un `buckets` tableau. Le tableau contient un objet pour chaque compartiment figurant dans

le compartiment actuel Région AWS et correspondant aux critères du filtre. Pour un exemple de ce résultat, développez la section suivante.

Exemple de **`buckets`** tableau

Dans cet exemple, le `buckets` tableau fournit des détails sur deux compartiments qui correspondent aux critères de filtre spécifiés dans une requête.


```
{
    "buckets": [
        {
            "accountId": "123456789012",
            "allowsUnencryptedObjectUploads": "FALSE",
            "automatedDiscoveryMonitoringStatus": "MONITORED",
            "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
            "bucketCreatedAt": "2020-05-18T19:54:00+00:00",
            "bucketName": "DOC-EXAMPLE-BUCKET1",
            "classifiableObjectCount": 13,
            "classifiableSizeInBytes": 1592088,
            "jobDetails": {
                "isDefinedInJob": "TRUE",
                "isMonitoredByJob": "TRUE",
                "lastJobId": "08c81dc4a2f3377fae45c9ddaexample",
                "lastJobRunTime": "2024-05-26T14:55:30.270000+00:00"
            },
            "lastAutomatedDiscoveryTime": "2024-06-07T19:11:25.364000+00:00",
            "lastUpdated": "2024-06-12T07:33:06.337000+00:00",
            "objectCount": 13,
            "objectCountByEncryptionType": {
                "customerManaged": 0,
                "kmsManaged": 2,
                "s3Managed": 7,
                "unencrypted": 4,
                "unknown": 0
            },
            "publicAccess": {
                "effectivePermission": "NOT_PUBLIC",
                "permissionConfiguration": {
                    "accountLevelPermissions": {
                        "blockPublicAccess": {
                            "blockPublicAcls": true,
                            "blockPublicPolicy": true,
                            "ignorePublicAcls": true,
```

```
                        "restrictPublicBuckets": true
                    }
                },
                "bucketLevelPermissions": {
                    "accessControlList": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    },
                    "blockPublicAccess": {
                        "blockPublicAcls": true,
                        "blockPublicPolicy": true,
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true
                    },
                    "bucketPolicy": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    }
                }
            },
            "region": "us-east-1",
            "replicationDetails": {
                "replicated": false,
                "replicatedExternally": false,
                "replicationAccounts": []
            },
            "sensitivityScore": 78,
            "serverSideEncryption": {
                "kmsMasterKeyId": null,
                "type": "NONE"
            },
            "sharedAccess": "NOT_SHARED",
            "sizeInBytes": 4549746,
            "sizeInBytesCompressed": 0,
            "tags": [
                {
                    "key": "Division",
                    "value": "HR"
                },
                {
                    "key": "Team",
                    "value": "Recruiting"
                }
```

```
            ],
            "unclassifiableObjectCount": {
                "fileType": 0,
                "storageClass": 0,
                "total": 0
            },
            "unclassifiableObjectSizeInBytes": {
                "fileType": 0,
                "storageClass": 0,
                "total": 0
            },
            "versioning": true
        },
        {
            "accountId": "123456789012",
            "allowsUnencryptedObjectUploads": "TRUE",
            "automatedDiscoveryMonitoringStatus": "MONITORED",
            "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
            "bucketCreatedAt": "2020-11-25T18:24:38+00:00",
            "bucketName": "DOC-EXAMPLE-BUCKET2",
            "classifiableObjectCount": 8,
            "classifiableSizeInBytes": 133810,
            "jobDetails": {
                "isDefinedInJob": "TRUE",
                "isMonitoredByJob": "FALSE",
                "lastJobId": "188d4f6044d621771ef7d65f2example",
                "lastJobRunTime": "2024-04-09T19:37:11.511000+00:00"
            },
            "lastAutomatedDiscoveryTime": "2024-06-07T19:11:25.364000+00:00",
            "lastUpdated": "2024-06-12T07:33:06.337000+00:00",
            "objectCount": 8,
            "objectCountByEncryptionType": {
                "customerManaged": 0,
                "kmsManaged": 0,
                "s3Managed": 8,
                "unencrypted": 0,
                "unknown": 0
            },
            "publicAccess": {
                "effectivePermission": "NOT_PUBLIC",
                "permissionConfiguration": {
                    "accountLevelPermissions": {
                        "blockPublicAccess": {
                            "blockPublicAcls": true,
```

```
                        "blockPublicPolicy": true,
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true
                    }
                },
                "bucketLevelPermissions": {
                    "accessControlList": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    },
                    "blockPublicAccess": {
                        "blockPublicAcls": true,
                        "blockPublicPolicy": true,
                        "ignorePublicAcls": true,
                        "restrictPublicBuckets": true
                    },
                    "bucketPolicy": {
                        "allowsPublicReadAccess": false,
                        "allowsPublicWriteAccess": false
                    }
                }
            }
        },
        "region": "us-east-1",
        "replicationDetails": {
            "replicated": false,
            "replicatedExternally": false,
            "replicationAccounts": []
        },
        "sensitivityScore": 95,
        "serverSideEncryption": {
            "kmsMasterKeyId": null,
            "type": "AES256"
        },
        "sharedAccess": "EXTERNAL",
        "sizeInBytes": 175978,
        "sizeInBytesCompressed": 0,
        "tags": [
            {
                "key": "Division",
                "value": "HR"
            },
            {
                "key": "Team",
```

```
                    "value": "Recruiting"
                }
            ],
            "unclassifiableObjectCount": {
                "fileType": 3,
                "storageClass": 0,
                "total": 3
            },
            "unclassifiableObjectSizeInBytes": {
                "fileType": 2999826,
                "storageClass": 0,
                "total": 2999826
            },
            "versioning": true
        }
    ]
}
```

Si aucun compartiment ne correspond aux critères du filtre, Macie renvoie un tableau vide. `buckets`

```
{
    "buckets": []
}
```

Exemple 1 : Rechercher des compartiments par nom de compartiment

Cet exemple utilise la commande describe-buckets pour interroger les métadonnées de tous les compartiments dont le nom commence par My-S3 et se trouve dans le répertoire current. Région AWS

Pour Linux, macOS ou Unix :

```
$ aws macie2 describe-buckets --criteria '{"bucketName":{"prefix":"my-S3"}}'
```

Pour Microsoft Windows :

```
C:\> aws macie2 describe-buckets --criteria={\"bucketName\":{\"prefix\":\"my-S3\"}}
```

Où :

- *`BucketName`* spécifie le nom JSON du champ Bucket name.
- *`prefix`* spécifie l'opérateur de préfixe.

- *My-S3* est la valeur du champ Nom du compartiment.

Exemple 2 : trouver des compartiments accessibles au public

Cet exemple utilise la commande describe-buckets pour interroger les métadonnées des buckets qui se trouvent dans la version actuelle Région AWS et qui, sur la base d'une combinaison de paramètres d'autorisation, sont accessibles au public.

Pour Linux, macOS ou Unix :

```
$ aws macie2 describe-buckets --criteria '{"publicAccess.effectivePermission":{"eq":["PUBLIC"]}}'
```

Pour Microsoft Windows :

```
C:\> aws macie2 describe-buckets --criteria={\"publicAccess.effectivePermission\":{\"eq\":[\"PUBLIC\"]}}
```

Où :

- *PublicAccess.EffectivePermission spécifie le nom JSON du champ d'autorisation* effective.
- *eq* spécifie l'opérateur égal.
- *PUBLIC* est une valeur énumérée pour le champ Autorisation effective.

Exemple 3 : Rechercher des compartiments contenant des objets non chiffrés

Cet exemple utilise la commande describe-buckets pour interroger les métadonnées des buckets qui se trouvent dans les compartiments actuels Région AWS et qui stockent des objets non chiffrés.

Pour Linux, macOS ou Unix :

```
$ aws macie2 describe-buckets --criteria '{"objectCountByEncryptionType.unencrypted":{"gte":1}}'
```

Pour Microsoft Windows :

```
C:\> aws macie2 describe-buckets --criteria={\"objectCountByEncryptionType.unencrypted\":{\"gte\":1}}
```

Où :

- *objectCountByEncryptionType.unencrypted* spécifie le nom JSON du champ No encryption.
- *gte* spécifie l'opérateur supérieur ou égal à.
- *1* est la valeur la plus faible d'une plage numérique relative inclusive pour le champ Aucun chiffrement.

Exemple 4 : Rechercher des compartiments qui ne sont pas surveillés par une tâche

Cet exemple utilise la commande describe-buckets pour interroger les métadonnées des buckets qui se trouvent dans le répertoire actuel Région AWS et qui ne sont associés à aucune tâche périodique de découverte de données sensibles.

Pour Linux, macOS ou Unix :

```
$ aws macie2 describe-buckets --criteria '{"jobDetails.isMonitoredByJob":{"eq":
["FALSE"]}}'
```

Pour Microsoft Windows :

```
C:\> aws macie2 describe-buckets --criteria={\"jobDetails.isMonitoredByJob\":{\"eq\":
[\"FALSE\"]}}
```

Où :

- *Détails du poste. isMonitoredByJob* spécifie le nom JSON du champ Activement surveillé par tâche.
- *eq* spécifie l'opérateur égal.
- *FALSE* est une valeur énumérée pour le champ Surveillance active par tâche.

Exemple 5 : trouver des compartiments qui répliquent les données vers des comptes externes

Cet exemple utilise la commande describe-buckets pour interroger les métadonnées des buckets qui se trouvent dans le répertoire actuel Région AWS et qui sont configurés pour répliquer des objets vers un compartiment ne Compte AWS faisant pas partie de votre organisation.

Pour Linux, macOS ou Unix :

```
$ aws macie2 describe-buckets --criteria '{"replicationDetails.replicatedExternally":
{"eq":["true"]}}'
```

Pour Microsoft Windows :

```
C:\> aws macie2 describe-buckets --
criteria={\"replicationDetails.replicatedExternally\":{\"eq\":[\"true\"]}}
```

Où :

- *ReplicationDetails.ReplicatedExternally spécifie le nom JSON du champ Replicated externally*.
- *eq* spécifie l'opérateur égal.
- *true* spécifie une valeur booléenne pour le champ externe répliqué.

Exemple 6 : Rechercher des compartiments en fonction de plusieurs critères

Cet exemple utilise la commande describe-buckets pour interroger les métadonnées des buckets qui se trouvent dans le répertoire actuel Région AWS et répondent aux critères suivants : ils sont accessibles au public en fonction d'une combinaison de paramètres d'autorisation ; ils stockent des objets non chiffrés ; et ils ne sont associés à aucune tâche périodique de découverte de données sensibles.

Pour Linux, macOS ou Unix, utilisez la barre oblique inverse (\) pour améliorer la lisibilité :

```
$ aws macie2 describe-buckets \
--criteria '{"publicAccess.effectivePermission":{"eq":
["PUBLIC"]},"objectCountByEncryptionType.unencrypted":
{"gte":1},"jobDetails.isMonitoredByJob":{"eq":["FALSE"]}}'
```

Pour Microsoft Windows, utilisez le caractère de continuation de ligne caret (^) pour améliorer la lisibilité :

```
C:\> aws macie2 describe-buckets ^
--criteria={\"publicAccess.effectivePermission\":{\"eq\":
[\"PUBLIC\"]},\"objectCountByEncryptionType.unencrypted\":{\"gte\":1},
\"jobDetails.isMonitoredByJob\":{\"eq\":[\"FALSE\"]}}
```

Où :

- *PublicAccess.EffectivePermission spécifie le nom JSON du champ d'autorisation* effective et :
  - *eq* spécifie l'opérateur égal.
  - *PUBLIC* est une valeur énumérée pour le champ Autorisation effective.
- *objectCountByEncryptionType.unencrypted* spécifie le nom JSON du champ No encryption, et :
  - *gte* spécifie l'opérateur supérieur ou égal à.
  - *1* est la valeur la plus faible d'une plage numérique relative inclusive pour le champ Aucun chiffrement.
- *Détails du poste. isMonitoredByJob* spécifie le nom JSON du champ Activement surveillé par tâche, et :
  - *eq* spécifie l'opérateur égal.
  - *FALSE* est une valeur énumérée pour le champ Surveillance active par tâche.

Autoriser Amazon Macie à accéder aux compartiments et aux objets S3

Lorsque vous activez Amazon Macie pour votre compte Compte AWS, Macie crée un rôle lié à un service qui lui accorde les autorisations nécessaires pour appeler Amazon Simple Storage Service (Amazon S3) et d'autres personnes en votre nom. Services AWS Un rôle lié à un service simplifie le processus de configuration Service AWS car vous n'avez pas à ajouter manuellement des autorisations pour que le service puisse effectuer des actions en votre nom. Pour en savoir plus sur ce type de rôle, consultez la section Utilisation des rôles liés à un service dans le Guide de l'AWS Identity and Access Management utilisateur.

La politique d'autorisation pour le rôle lié au service Macie (`AWSServiceRoleForAmazonMacie`) permet à Macie d'effectuer des actions qui incluent la récupération d'informations sur vos compartiments et objets S3, ainsi que la récupération d'objets de vos compartiments. Si vous êtes l'administrateur Macie d'une organisation, la politique permet également à Macie d'effectuer ces actions en votre nom pour les comptes des membres de votre organisation.

Macie utilise ces autorisations pour effectuer des tâches telles que :

- Générez et maintenez un inventaire de vos buckets S3 à usage général

- Fournir des données statistiques et autres sur les compartiments et les objets qu'ils contiennent
- Surveillez et évaluez les compartiments à des fins de sécurité et de contrôle d'accès
- Analysez les objets dans les compartiments pour détecter les données sensibles

Dans la plupart des cas, Macie dispose des autorisations nécessaires pour effectuer ces tâches. Toutefois, si un compartiment S3 possède une politique de compartiment restrictive, cette politique peut empêcher Macie d'effectuer certaines ou toutes ces tâches.

Une politique de compartiment est une politique basée sur les ressources AWS Identity and Access Management (IAM) qui spécifie les actions qu'un principal (utilisateur, compte, service ou autre entité) peut effectuer sur un compartiment S3, ainsi que les conditions dans lesquelles un principal peut effectuer ces actions. Les actions et conditions peuvent s'appliquer aux opérations au niveau du compartiment, telles que la récupération d'informations sur un compartiment, et aux opérations au niveau des objets, telles que la récupération d'objets d'un compartiment.

Les politiques relatives aux compartiments accordent ou restreignent généralement l'accès en utilisant `Deny` des déclarations et des conditions explicites`Allow`. Par exemple, une politique de compartiment peut contenir une `Deny` déclaration `Allow` ou qui refuse l'accès au compartiment, sauf si des adresses IP source spécifiques, des points de terminaison Amazon Virtual Private Cloud (Amazon VPC) ou des VPC sont utilisés pour accéder au compartiment. Pour plus d'informations sur l'utilisation des politiques relatives aux compartiments pour accorder ou restreindre l'accès aux compartiments, consultez les sections Politiques relatives aux compartiments et politiques utilisateur et Comment Amazon S3 autorise une demande dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Si une politique de compartiment utilise une `Allow` déclaration explicite, elle n'empêche pas Macie de récupérer des informations sur le compartiment et les objets du compartiment, ou de récupérer des objets du compartiment. Cela est dû au fait que les `Allow` instructions de la politique d'autorisation pour le rôle lié au service Macie accordent ces autorisations.

Toutefois, si une politique de compartiment utilise une `Deny` déclaration explicite assortie d'une ou plusieurs conditions, Macie peut ne pas être autorisée à récupérer des informations sur le compartiment ou les objets du compartiment, ou à récupérer les objets du compartiment. Par exemple, si une politique de bucket refuse explicitement l'accès à toutes les sources à l'exception d'une adresse IP spécifique, Macie ne sera pas autorisé à analyser les objets du bucket lorsque vous exécutez une tâche de découverte de données sensibles. Cela est dû au fait que les politiques de compartiment restrictives ont priorité sur les `Allow` instructions de la politique d'autorisation pour le rôle lié au service Macie.

Pour permettre à Macie d'accéder à un compartiment S3 doté d'une politique de compartiment restrictive, vous pouvez ajouter une condition pour le rôle lié au service Macie (`AWSServiceRoleForAmazonMacie`) à la politique de compartiment. La condition peut empêcher le rôle lié au service Macie de correspondre à la `Deny` restriction de la politique. Il peut le faire en utilisant la clé de contexte de condition `aws:PrincipalArn` globale et le nom de ressource Amazon (ARN) du rôle lié au service Macie.

La procédure suivante vous guide tout au long de ce processus et fournit un exemple.

Pour ajouter le rôle lié au service Macie à une politique de compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Compartiments.
3. Choisissez le compartiment S3 auquel vous souhaitez autoriser Macie à accéder.
4. Dans l'onglet Permissions (Autorisations), sous Bucket Policy (Stratégie de compartiment), choisissez Edit (Modifier).
5. Dans l'éditeur de politique de bucket, identifiez chaque `Deny` instruction qui restreint l'accès et empêche Macie d'accéder au bucket ou aux objets du bucket.
6. Dans chaque `Deny` instruction, ajoutez une condition qui utilise la clé de contexte de condition `aws:PrincipalArn` globale et spécifie l'ARN du rôle lié au service Macie pour votre. Compte AWS

   La valeur de la clé de condition doit être`arn:aws:iam::123456789012:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`, où *123456789012* est l'identifiant de compte de votre. Compte AWS

L'endroit où vous l'ajoutez à une politique de compartiment dépend de la structure, des éléments et des conditions que la politique contient actuellement. Pour en savoir plus sur les structures et les éléments pris en charge, consultez la section Politiques et autorisations dans Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Voici un exemple de politique de compartiment qui utilise une `Deny` instruction explicite pour restreindre l'accès à un compartiment S3 nommé DOC-EXAMPLE-BUCKET. Avec la politique actuelle, le bucket n'est accessible qu'à partir du point de terminaison VPC dont l'ID est. `vpce-1a2b3c4d` L'accès depuis tous les autres points de terminaison VPC est refusé, y compris l'accès depuis Macie et Macie. AWS Management Console

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115example",
   "Statement": [
      {
         "Sid": "Access from specific VPCE only",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "s3:*",
         "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
         ],
         "Condition": {
            "StringNotEquals": {
               "aws:SourceVpce": "vpce-1a2b3c4d"
            }
         }
      }
   ]
}
```

Pour modifier cette politique et permettre à Macie d'accéder au compartiment S3 et aux objets du compartiment, nous pouvons ajouter une condition qui utilise l'opérateur de `StringNotLike` condition et la clé de contexte de condition `aws:PrincipalArn` globale. Cette condition supplémentaire empêche le rôle lié au service Macie de correspondre à la restriction. `Deny`

```
{
   "Version": "2012-10-17",
   "Id":" Policy1415115example ",
   "Statement": [
      {
         "Sid": "Access from specific VPCE and Macie only",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "s3:*",
         "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
         ],
         "Condition": {
            "StringNotEquals": {
```

```
                "aws:SourceVpce": "vpce-1a2b3c4d"
            },
            "StringNotLike": {
                "aws:PrincipalArn": "arn:aws:iam::123456789012:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
            }
         }
      }
   ]
}
```

Dans l'exemple précédent, l'opérateur de `StringNotLike` condition utilise la clé de contexte de `aws:PrincipalArn` condition pour spécifier l'ARN du rôle lié au service Macie, où :

- `123456789012`est l'ID de compte de la Compte AWS personne autorisée à utiliser Macie pour récupérer des informations sur le bucket et les objets du bucket, ainsi que pour récupérer des objets du bucket.
- `macie.amazonaws.com`est l'identifiant du principal de service Macie.
- `AWSServiceRoleForAmazonMacie`est le nom du rôle lié au service Macie.

Nous avons utilisé l'`StringNotLike`opérateur parce que la politique utilise déjà un `StringNotEquals` opérateur. Une politique ne peut utiliser l'`StringNotEquals`opérateur qu'une seule fois.

Pour des exemples de politiques supplémentaires et des informations détaillées sur la gestion de l'accès aux ressources Amazon S3, consultez la section Gestion des identités et des accès dans Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Découvrir des données sensibles avec Amazon Macie

Avec Amazon Macie, vous pouvez automatiser la découverte, la journalisation et le reporting des données sensibles dans votre parc de données Amazon Simple Storage Service (Amazon S3). Vous pouvez le faire de deux manières : en configurant Macie pour effectuer la découverte automatique des données sensibles, et en créant et en exécutant des tâches de découverte de données sensibles.

Découverte automatisée des données sensibles

> La découverte automatisée des données sensibles fournit une visibilité étendue sur l'emplacement des données sensibles susceptibles de se trouver dans votre parc de données Amazon S3. Avec cette option, Macie évalue quotidiennement votre inventaire de compartiments S3 et utilise des techniques d'échantillonnage pour identifier et sélectionner des objets S3 représentatifs de vos compartiments. Macie récupère et analyse ensuite les objets sélectionnés, en les inspectant pour détecter la présence de données sensibles. Pour plus d’informations, consultez Réalisation de la découverte automatisée des données sensibles.

Jobs de découverte de données sensibles

> Les tâches de découverte de données sensibles permettent une analyse plus approfondie et plus ciblée. Cette option vous permet de définir l'étendue et la profondeur de l'analyse, qu'il s'agisse de compartiments S3 spécifiques que vous sélectionnez ou de compartiments répondant à des critères spécifiques. Vous pouvez également affiner la portée de l'analyse en choisissant des options telles que des critères personnalisés dérivés des propriétés des objets S3. En outre, vous pouvez configurer une tâche pour qu'elle ne soit exécutée qu'une seule fois pour une analyse et une évaluation à la demande, ou de manière récurrente pour une analyse, une évaluation et une surveillance périodiques. Pour plus d’informations, consultez Exécution de tâches de découverte de données sensibles.

Quelle que soit l'option, qu'il s'agisse de découverte automatique de données sensibles ou de tâches de découverte de données sensibles, vous pouvez analyser des objets S3 à l'aide d'identifiants de données gérés fournis par Macie, d'identifiants de données personnalisés que vous définissez ou d'une combinaison des deux. Vous pouvez également affiner l'analyse en utilisant des listes d'autorisation.

Identifiants de données gérés

Les identifiants de données gérés sont des critères et des techniques intégrés conçus pour détecter des types spécifiques de données sensibles, par exemple, les numéros de carte de crédit, les clés d'accès AWS secrètes ou les numéros de passeport pour certains pays ou régions. Ils peuvent détecter une liste longue et croissante de types de données sensibles pour de nombreux pays et régions, notamment plusieurs types de données d'identification, d'informations financières et d'informations personnelles identifiables (PII). Pour plus d'informations, consultez Utilisation des identificateurs de données gérés.

Identifiants de données personnalisés

Les identificateurs de données personnalisés définissent des critères personnalisés pour détecter les données sensibles. Chaque identifiant de données personnalisé spécifie une expression régulière (regex) qui définit un modèle de texte correspondant et, éventuellement, des séquences de caractères et une règle de proximité qui affinent les résultats. Vous pouvez les utiliser pour détecter les données sensibles qui reflètent vos scénarios particuliers, les données de propriété intellectuelle ou les données propriétaires, par exemple les identifiants des employés, les numéros de compte client ou les classifications de données internes. Pour plus d'informations, consultez Création d'identificateurs de données personnalisés.

Autoriser les listes

Dans Macie, les listes d'autorisations spécifient le texte et les modèles de texte à ignorer dans les objets S3, généralement des exceptions de données sensibles pour vos scénarios ou votre environnement particuliers, par exemple les noms publics ou les numéros de téléphone de votre organisation, ou des exemples de données que votre organisation utilise pour les tests. Si Macie trouve du texte correspondant à une entrée ou à un modèle dans une liste d'autorisation, Macie ne signale pas cette occurrence de texte, même si le texte répond aux critères d'un identifiant de données géré ou d'un identifiant de données personnalisé. Pour plus d'informations, consultez Définition des exceptions relatives aux données sensibles à l'aide de listes d'autorisation.

Lorsque Macie analyse un objet S3, Macie récupère la dernière version de l'objet auprès d'Amazon S3, puis inspecte le contenu de l'objet pour détecter la présence de données sensibles. Macie peut analyser un objet si les conditions suivantes sont vraies :

- L'objet utilise un format de fichier ou de stockage pris en charge et il est stocké dans un compartiment S3 à usage général utilisant une classe de stockage prise en charge. Pour plus d'informations, consultez Classes et formats de stockage pris en charge.

- Si l'objet est chiffré, il est chiffré avec une clé à laquelle Macie peut accéder et est autorisée à utiliser. Pour plus d'informations, consultez Analyse des objets S3 chiffrés.
- Si l'objet est stocké dans un compartiment doté d'une politique de compartiment restrictive, cette politique permet à Macie d'accéder aux objets du compartiment. Pour plus d'informations, consultez Autoriser Macie à accéder aux compartiments et aux objets S3.

Pour vous aider à respecter et à maintenir la conformité à vos exigences en matière de sécurité et de confidentialité des données, Macie enregistre les données sensibles qu'elle trouve et les analyses qu'elle effectue, c'est-à-dire les découvertes de données sensibles et les résultats de découverte de données sensibles. Une découverte de données sensibles est un rapport détaillé des données sensibles que Macie a trouvées dans un objet S3. Un résultat de découverte de données sensibles est un enregistrement qui consigne les détails de l'analyse d'un objet. Chaque type d'enregistrement adhère à un schéma standardisé, qui peut vous aider à les interroger, à les surveiller et à les traiter en utilisant d'autres applications, services et systèmes si nécessaire.

> **Tip**
>
> Bien que Macie soit optimisé pour Amazon S3, vous pouvez l'utiliser pour découvrir des données sensibles dans des ressources que vous stockez actuellement ailleurs. Vous pouvez le faire en déplaçant les données vers Amazon S3 de manière temporaire ou permanente. Par exemple, exportez des instantanés Amazon Relational Database Service ou Amazon Aurora vers Amazon S3 au format Apache Parquet. Ou exportez une table Amazon DynamoDB vers Amazon S3. Vous pouvez ensuite créer une tâche pour analyser les données dans Amazon S3.

Rubriques

- Classes et formats de stockage pris en charge par Amazon Macie

Utilisation d'identifiants de données gérés dans Amazon Macie

Amazon Macie utilise une combinaison de critères et de techniques, notamment l'apprentissage automatique et la mise en correspondance de modèles, pour détecter les données sensibles dans les objets Amazon Simple Storage Service (Amazon S3). Ces critères et techniques, collectivement dénommésidentifiants de données gérés, peut détecter une liste longue et croissante de types de données sensibles pour de nombreux pays et régions, notamment de multiples types de données d'identification, d'informations financières, d'informations personnelles sur la santé (PHI) et d'informations personnelles identifiables (PII). Chaque identifiant de données gérées est conçu pour détecter un type spécifique de données sensibles, par exemple,AWSles clés d'accès secrètes, les numéros de carte de crédit ou les numéros de passeport d'un pays ou d'une région en particulier.

Macie peut détecter les catégories de données sensibles suivantes à l'aide d'identifiants de données gérés :

- Informations d'identification, pour les données d'identification telles que les clés privées etAWSclés d'accès secrètes.
- Informations financières, pour les données financières telles que les numéros de carte de crédit et les numéros de comptes bancaires.
- Informations personnelles, pour les PHI tels que les numéros d'assurance maladie et d'identification médicale, et les informations personnelles telles que les numéros d'identification du permis de conduire et les numéros de passeport.

Dans chaque catégorie, Macie peut détecter plusieurs types de données sensibles. Les rubriques de cette section répertorient et décrivent chaque type ainsi que toutes les exigences pertinentes pour le détecter. Pour chaque type, elles indiquent également l'identifiant unique (ID) de l'identifiant de données gérées conçu pour détecter les données. Quand tucréer une tâche de découverte de données sensiblesouconfigurer les paramètres de découverte automatique des données sensibles, vous pouvez utiliser ces identifiants pour spécifier les identifiants de données gérées que vous souhaitez que Macie utilise lorsqu'elle analyse des objets S3.

Pour obtenir la liste des identifiants de données gérés que nous recommandons pour les tâches, voirIdentificateurs de données gérés recommandés pour les tâches de découverte de données sensibles. Pour obtenir la liste des identifiants de données gérés que nous recommandons et qui sont

utilisés par défaut pour la découverte automatique de données sensibles, voirParamètres par défaut pour la découverte automatique des données sensibles.

Rubriques

- Exigences relatives aux mots clés pour les identifiants de données gérés par Amazon Macie
- Référence rapide : identifiants de données gérés par Amazon Macie
- Référence détaillée : Identifiants de données gérés par Amazon Macie

Exigences relatives aux mots clés pour les identifiants de données gérés par Amazon Macie

Pour détecter certains types de données sensibles à l'aide d'identifiants de données gérés, Amazon Macie a besoin qu'un mot clé se trouve à proximité des données. Si tel est le cas pour un type de données particulier, les rubriques suivantes de cette section indiquent les exigences relatives aux mots clés pour ces données.

Si un mot clé doit se trouver à proximité d'un type de données particulier, il doit généralement se trouver à moins de 30 caractères (inclus) des données. Les exigences de proximité supplémentaires varient en fonction du type de fichier ou du format de stockage d'un objet Amazon Simple Storage Service (Amazon S3).

Données structurées en colonnes

Pour les données en colonnes, un mot clé doit faire partie de la même valeur ou figurer dans le nom de la colonne ou du champ qui stocke une valeur. Cela est vrai pour les classeurs Microsoft Excel, les fichiers CSV et les fichiers TSV.

Par exemple, si la valeur d'un champ contient les deuxSSNet un numéro à neuf chiffres qui utilise la syntaxe d'un numéro de sécurité sociale (SSN) américain, Macie peut détecter le SSN sur le terrain. De même, si le nom d'une colonne contientSSN, Macie peut détecter chaque SSN de la colonne. Macie considère les valeurs de cette colonne comme étant proches du mot cléSSN.

Données structurées basées sur des enregistrements

Pour les données basées sur des enregistrements, un mot clé doit faire partie de la même valeur ou figurer dans le nom d'un élément du chemin d'accès au champ ou au tableau qui stocke une valeur. Cela est vrai pour les conteneurs d'objets Apache Avro, les fichiers Apache Parquet, les fichiers JSON et les fichiers JSON Lines.

Par exemple, si la valeur d'un champ contient les deuxinformations d'identificationet une séquence de caractères qui utilise la syntaxe d'unAWSclé d'accès secrète, Macie peut détecter la clé sur le terrain. De même, si le chemin d'accès à un champ est`$.credentials.aws.key`, Macie peut détecter unAWSclé d'accès secrète sur le terrain. Macie considère que la valeur du champ se trouve à proximité du mot cléinformations d'identification.

Données non structurées

Il n'existe aucune exigence de proximité supplémentaire pour les fichiers Adobe Portable Document Format, les documents Microsoft Word, les messages électroniques et les fichiers texte non binaires autres que les fichiers CSV, JSON, JSON Lines et TSV. Un mot clé doit généralement se trouver dans un rayon de 30 caractères (inclus) des données. Cela inclut toutes les données structurées, telles que les tables, présentes dans ces types de fichiers.

Les mots clés ne sont pas sensibles à la casse. En outre, si un mot clé contient un espace, Macie fait automatiquement correspondre les variantes de mot clé qui ne contiennent pas d'espace ou qui contiennent un trait de soulignement (_) ou un trait d'union (-) à la place de l'espace. Dans certains cas, Macie développe ou abrége également un mot clé pour traiter des variantes courantes du mot clé.

Pour une démonstration de la manière dont les mots clés fournissent du contexte et aident Macie à détecter des types spécifiques de données sensibles, regardez la vidéo suivante :Comment Amazon Macie utilise des mots clés pour découvrir des données sensibles.

Référence rapide : identifiants de données gérés par Amazon Macie

Dans Amazon Macie, un identifiant de données géré est un ensemble de critères et de techniques intégrés conçus pour détecter un type spécifique de données sensibles, par exemple les numéros de carte de crédit, les clés d'accès AWS secrètes ou les numéros de passeport d'un pays ou d'une région en particulier. Ces identifiants peuvent détecter une liste longue et croissante de types de données sensibles pour de nombreux pays et régions, notamment plusieurs types de données d'identification, d'informations financières, d'informations médicales personnelles (PHI) et d'informations personnelles identifiables (PII).

Le tableau suivant répertorie tous les identifiants de données gérés actuellement fournis par Macie, organisés par type de données sensibles. Pour chaque type, il fournit les informations suivantes :

- Catégorie de données sensibles — Spécifie la catégorie générale de données sensibles qui inclut le type : informations d'identification, pour les données d'identification telles que les clés privées ; informations financières, pour les données financières telles que les numéros de carte de crédit et les numéros de compte bancaire ; informations personnelles : informations personnelles : informations personnelles telles que les numéros d'identification du permis de conduire et numéros de passeport.
- ID d'identifiant de données gérées — Spécifie l'identifiant unique (ID) pour un ou plusieurs identifiants de données gérées conçus pour détecter les données. Lorsque vous créez une tâche de découverte de données sensibles ou que vous configurez des paramètres de découverte automatique de données sensibles, vous pouvez utiliser ces identifiants pour spécifier les identifiants de données gérées que vous souhaitez que Macie utilise lors de l'analyse des données. Pour obtenir la liste des identifiants de données gérés que nous recommandons pour les tâches, consultezIdentificateurs de données gérés recommandés pour les tâches de découverte de données sensibles. Pour obtenir la liste des identifiants de données gérés que nous recommandons pour la découverte automatique de données sensibles, consultezParamètres par défaut pour la découverte automatique des données sensibles.
- Mot-clé obligatoire — Spécifie si la détection nécessite qu'un mot clé se trouve à proximité des données. Pour plus d'informations sur la façon dont Macie utilise les mots clés lorsqu'il analyse les données, consultezExigences relatives aux mots-clés.
- Pays et régions — Spécifie les pays ou régions pour lesquels les identifiants de données gérées applicables sont conçus. Si les identifiants de données gérés ne sont pas conçus pour des pays ou des régions spécifiques, cette valeur est Any.

Pour consulter des informations supplémentaires sur les identifiants de données gérés pour un type particulier de données sensibles, choisissez le type.

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Clé d'accès secrète AWS	Informations d'identification	AWS_CREDENTIALS	Oui	N'importe quel compte

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Numéro de compte bancaire	Informations financières	BANK_ACCOUNT_NUMBER(pour le Canada et les États-Unis)	Oui	Canada, États-Unis
Numéro de compte bancaire de base (BBAN)	Informations financières	En fonction du pays ou de la région : FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER	Oui	France, Allemagne, Italie, Espagne, Royaume-Uni
Date de naissance	Informations personnelles : PII	DATE_OF_BIRTH	Oui	N'importe quel compte
Date d'expiration de carte de crédit	Informations financières	CREDIT_CARD_EXPIRATION	Oui	N'importe quel compte
Données relatives à la bande magnétique des cartes de crédit	Informations financières	CREDIT_CARD_MAGNETIC_STRIPE	Oui	N'importe quel compte

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Numéro de carte de crédit	Informations financières	CREDIT_CARD_NUMBER(pour les numéros de carte de crédit situés à proximité d'un mot clé), CREDIT_CARD_NUMBER_(NO_KEYWORD) (pour les numéros de carte de crédit situés à proximité d'un mot clé)	Varie	N'importe quel compte
Code de vérification de carte de crédit	Informations financières	CREDIT_CARD_SECURITY_CODE	Oui	N'importe quel compte

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Numéro d'identification du permis de conduire	Informations personnelles : PII	En fonction du pays ou de la région : AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICE	Oui	Australie, Autriche, Belgique, Bulgarie, Canada, Chypre, Croatie, République tchèque, Danemark, Estonie, Finlande, France, Allemagne, Grèce, Hongrie, Inde, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, Roumanie, Slovaquie, Slovénie, Espagne, Suède,

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		Royaume-Uni, États-Unis
Numéro d'enregistrement de la Drug Enforcement Agency (DEA)	Informations personnelles : PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	Oui	ETATS-UNIS
Numéro de liste électorale	Informations personnelles : PII	UK_ELECTORAL_ROLL_NUMBER	Oui	Royaume-Uni
Nom complet	Informations personnelles : PII	NAME	Non	N'importe lequel, si le nom utilise un jeu de caractères latins
Coordonnées du système de positionnement global (GPS)	Informations personnelles : PII	LATITUDE_LONGITUDE	Oui	N'importe lequel, si les coordonnées se trouvent à proximité d'un mot clé anglais

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Clé d'API Google Cloud	Informations d'identification	GCP_API_KEY	Oui	N'importe quel compte
Numéro de réclamation d'assurance maladie (HICN)	Informations personnelles : PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	Oui	ETATS-UNIS
Numéro d'assurance maladie ou d'identification médicale	Informations personnelles : PHI	En fonction du pays ou de la région : CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	Oui	Canada, UE, Finlande, France, Royaume-Uni, États-Unis

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Code du système de codage des procédures communes pour les soins de santé (HCPCS)	Informations personnelles : PHI	USA_HEALTHCARE_PROCEDURE_CODE	Oui	ETATS-UNIS
En-tête d'autorisation HTTP Basic	Informations d'identification	HTTP_BASIC_AUTH_HEADER	Non	N'importe quel compte
Cookie HTTP	Informations personnelles : PII	HTTP_COOKIE	Non	N'importe quel compte

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Numéro de compte bancaire international (IBAN)	Informations financières	En fonction du pays ou de la région : ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER,	Non	Albanie, Andorre, Bosnie-Herzégovine, Brésil, Bulgarie, Costa Rica, Chypre, Croatie, République tchèque, Danemark, République dominicaine, Égypte, Estonie, îles Féroé, Finlande, France, Géorgie, Allemagne, Grèce, Groenland, Hongrie, Islande, Irlande, Italie, Jordanie, Kosovo, Liechtens

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
		IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER,		tein, Lituanie, Malte, Mauritanie, Maurice, Monaco, Monténégro, Pays-Bas, Macédoine du Nord, Pologne, Portugal, Saint-Marin, Sénégal, Serbie, Slovaquie, Slovénie, Espagne, Suède, Suisse, Timor-Leste, Tunisie, Turquie, Royaume-Uni, Ukraine, Émirats arabes unis, îles Vierges

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
		TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER(pour les îles Vierges britanniques)		britanniques
Jeton Web JSON (JWT)	Informations d'identification	JSON_WEB_TOKEN	Non	N'importe quel compte
Adresse postale	Informations personnelles : PII	ADDRESS, BRAZIL_CEP_CODE (pour le Código de Endereçamento Postal du Brésil)	Varie	Australie, Brésil, Canada, France, Allemagne, Italie, Espagne, Royaume-Uni, États-Unis
Code national des médicaments (NDC)	Informations personnelles : PHI	USA_NATIONAL_DRUG_CODE	Oui	ETATS-UNIS

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Numéro d'identification nationale	Informations personnelles : PII	En fonction du pays ou de la région : BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	Oui	Allemagne, Brésil, Espagne, France, Inde, Italie
Numéro d'assurance nationale (NINO)	Informations personnelles : PII	UK_NATIONAL_INSURANCE_NUMBER	Oui	Royaume-Uni
Identifiant national du fournisseur (NPI)	Informations personnelles : PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	Oui	ETATS-UNIS
Clé privée OpenSSH	Informations d'identification	OPENSSH_PRIVATE_KEY	Non	N'importe quel compte

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Numéro de passeport	Informations personnelles : PII	En fonction du pays ou de la région : CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	Oui	Canada, France, Allemagne, Italie, Espagne, Royaume-Uni, États-Unis
Numéro de résidence permanente	Informations personnelles : PII	CANADA_NATIONAL_IDENTIFICATION_NUMBER	Oui	Canada
Clé privée PGP	Informations d'identification	PGP_PRIVATE_KEY	Non	N'importe quel compte
Phone number (Numéro de téléphone)	Informations personnelles : PII	En fonction du pays ou de la région : BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER	Varie	Brésil, Canada, France, Allemagne, Italie, Espagne, Royaume-Uni, États-Unis

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Clé privée selon la norme de cryptographie à clé publique (PKCS)	Informations d'identification	PKCS	Non	N'importe quel compte
Clé privée PuTTY	Informations d'identification	PUTTY_PRIVATE_KEY	Non	N'importe quel compte
Numéro d'assurance sociale (SIN)	Informations personnelles : PII	CANADA_SOCIAL_INSURANCE_NUMBER	Oui	Canada
Numéro de sécurité sociale (SSN)	Informations personnelles : PII	Selon le pays ou la région : SPAIN_SOCIAL_SECURITY_NUMBER USA_SOCIAL_SECURITY_NUMBER	Oui	Espagne, États-Unis
the section called "Clé d'API Stripe"	Informations d'identification	STRIPE_CREDENTIALS	Non	N'importe quel compte

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Numéro d'identification ou de référence du contribuable	Informations personnelles : PII	En fonction du pays ou de la région : AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER	Oui	Australie, Brésil, France, Allemagne, Inde, Italie, Espagne, Royaume-Uni, États-Unis
Identifiant unique de l'appareil (UDI)	Informations personnelles : PHI	MEDICAL_DEVICE_UDI	Oui	ETATS-UNIS

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Numéro d'identification du véhicule (VIN)	Informations personnelles : PII	VEHICLE_IDENTIFICATION_NUMBER	Oui	N'importe lequel, si le VIN se trouve à proximité d'un mot clé dans l'une des langues suivantes : anglais, français, allemand, lituanien, polonais, portugais, roumain ou espagnol

Référence détaillée : Identifiants de données gérés par Amazon Macie

Dans Amazon Macie, les identifiants de données gérés sont des critères et des techniques intégrés conçus pour détecter des types spécifiques de données sensibles. Ils peuvent détecter une liste longue et croissante de types de données sensibles pour de nombreux pays et régions, notamment plusieurs types de données d'identification, d'informations financières et d'informations personnelles. Chaque identifiant de données géré est conçu pour détecter un type spécifique de données sensibles, par exemple des clés d'accès AWS secrètes, des numéros de carte de crédit ou des numéros de passeport pour un pays ou une région en particulier.

Macie peut détecter plusieurs catégories de données sensibles à l'aide d'identifiants de données gérés. Dans chaque catégorie, Macie peut détecter plusieurs types de données sensibles. Les

rubriques de cette section répertorient et décrivent chaque type ainsi que les exigences pertinentes pour détecter les données. Pour plus de détails sur les identifiants de données gérés pour des types spécifiques de données sensibles, vous pouvez parcourir les rubriques par catégorie :

- Informations d'identification — Pour les données d'identification telles que les clés privées et les clés d'accès AWS secrètes.
- Informations financières — Pour les données financières telles que les numéros de carte de crédit et les numéros de compte bancaire.
- Informations personnelles : PHI — Pour les informations médicales personnelles (PHI) telles que les numéros d'assurance maladie et d'identification médicale.
- Informations personnelles : PII — Pour les informations personnelles identifiables (PII) telles que les numéros d'identification du permis de conduire et les numéros de passeport.

Vous pouvez également sélectionner un type spécifique de données sensibles dans le tableau suivant. Le tableau répertorie tous les identifiants de données gérés actuellement fournis par Macie, organisés par type de données sensibles. Le tableau résume également les exigences pertinentes pour détecter chaque type.

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Clé d'accès secrète AWS	Informations d'identification	AWS_CREDENTIALS	Oui	N'importe quel compte
Numéro de compte bancaire	Informations financières	BANK_ACCOUNT_NUMBER(pour le Canada et les États-Unis)	Oui	Canada, États-Unis
Numéro de compte bancaire de base (BBAN)	Informations financières	Selon le pays ou la région : FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BAN	Oui	France, Allemagne, Italie, Espagne,

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
		K_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER		Royaume-Uni
Date de naissance	Informations personnelles : PII	DATE_OF_BIRTH	Oui	N'importe quel compte
Date d'expiration de carte de crédit	Informations financières	CREDIT_CARD_EXPIRATION	Oui	N'importe quel compte
Données relatives à la bande magnétique des cartes de crédit	Informations financières	CREDIT_CARD_MAGNETIC_STRIPE	Oui	N'importe quel compte
Numéro de carte de crédit	Informations financières	CREDIT_CARD_NUMBER(pour les numéros de carte de crédit situés à proximité d'un mot clé), CREDIT_CARD_NUMBER_(NO_KEYWORD) (pour les numéros de carte de crédit situés à proximité d'un mot clé)	Varie	N'importe quel compte
Code de vérification de carte de crédit	Informations financières	CREDIT_CARD_SECURITY_CODE	Oui	N'importe quel compte

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Numéro d'identification du permis de conduire	Informations personnelles : PII	Selon le pays ou la région : AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICE	Oui	Australie, Autriche, Belgique, Bulgarie, Canada, Chypre, Croatie, République tchèque, Danemark, Estonie, Finlande, France, Allemagne, Grèce, Hongrie, Inde, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, Roumanie, Slovaquie, Slovénie, Espagne, Suède,

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
		NSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE		Royaume-Uni, États-Unis
Numéro d'enregistrement de la Drug Enforcement Agency (DEA)	Informations personnelles : PHI	US_DRUG_ENFORCEMENT_AGENCY_NUMBER	Oui	ETATS-UNIS
Numéro de liste électorale	Informations personnelles : PII	UK_ELECTORAL_ROLL_NUMBER	Oui	Royaume-Uni
Nom complet	Informations personnelles : PII	NAME	Non	N'importe lequel, si le nom utilise un jeu de caractères latins
Coordonnées du système de positionnement global (GPS)	Informations personnelles : PII	LATITUDE_LONGITUDE	Oui	N'importe lequel, si les coordonnées se trouvent à proximité d'un mot clé anglais

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Clé d'API Google Cloud	Informations d'identification	GCP_API_KEY	Oui	N'importe quel compte
Numéro de réclamation d'assurance maladie (HICN)	Informations personnelles : PHI	USA_HEALTH_INSURANCE_CLAIM_NUMBER	Oui	ETATS-UNIS
Numéro d'assurance maladie ou d'identification médicale	Informations personnelles : PHI	Selon le pays ou la région : CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER	Oui	Canada, UE, Finlande, France, Royaume-Uni, États-Unis

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Code du système de codage des procédures communes pour les soins de santé (HCPCS)	Informations personnelles : PHI	USA_HEALTHCARE_PROCEDURE_CODE	Oui	ETATS-UNIS
En-tête d'autorisation HTTP Basic	Informations d'identification	HTTP_BASIC_AUTH_HEADER	Non	N'importe quel compte
Cookie HTTP	Informations personnelles : PII	HTTP_COOKIE	Non	N'importe quel compte

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Numéro de compte bancaire international (IBAN)	Informations financières	Selon le pays ou la région : ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER,	Non	Albanie, Andorre, Bosnie-Herzégovine, Brésil, Bulgarie, Costa Rica, Chypre, Croatie, République tchèque, Danemark, République dominicaine, Égypte, Estonie, îles Féroé, Finlande, France, Géorgie, Allemagne, Grèce, Groenland, Hongrie, Islande, Irlande, Italie, Jordanie, Kosovo, Liechtens

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
		IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER,		tein, Lituanie, Malte, Mauritanie, Maurice, Monaco, Monténégro, Pays-Bas, Macédoine du Nord, Pologne, Portugal, Saint-Marin, Sénégal, Serbie, Slovaquie, Slovénie, Espagne, Suède, Suisse, Timor-Leste, Tunisie, Turquie, Royaume-Uni, Ukraine, Émirats arabes unis, îles Vierges

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
		TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER(pour les îles Vierges britanniques)		britanniques
Jeton Web JSON (JWT)	Informations d'identification	JSON_WEB_TOKEN	Non	N'importe quel compte
Adresse postale	Informations personnelles : PII	ADDRESS, BRAZIL_CEP_CODE (pour le Código de Endereçamento Postal du Brésil)	Varie	Australie, Brésil, Canada, France, Allemagne, Italie, Espagne, Royaume-Uni, États-Unis
Code national des médicaments (NDC)	Informations personnelles : PHI	USA_NATIONAL_DRUG_CODE	Oui	ETATS-UNIS

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Numéro d'identification nationale	Informations personnelles : PII	Selon le pays ou la région : BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER	Oui	Allemagne, Brésil, Espagne, France, Inde, Italie
Numéro d'assurance nationale (NINO)	Informations personnelles : PII	UK_NATIONAL_INSURANCE_NUMBER	Oui	Royaume-Uni
Identifiant national du fournisseur (NPI)	Informations personnelles : PHI	USA_NATIONAL_PROVIDER_IDENTIFIER	Oui	ETATS-UNIS
Clé privée OpenSSH	Informations d'identification	OPENSSH_PRIVATE_KEY	Non	N'importe quel compte

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Numéro de passeport	Informations personnelles : PII	Selon le pays ou la région : CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER	Oui	Canada, France, Allemagne, Italie, Espagne, Royaume-Uni, États-Unis
Numéro de résidence permanente	Informations personnelles : PII	CANADA_NATIONAL_IDENTIFICATION_NUMBER	Oui	Canada
Clé privée PGP	Informations d'identification	PGP_PRIVATE_KEY	Non	N'importe quel compte
Phone number (Numéro de téléphone)	Informations personnelles : PII	Selon le pays ou la région : BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER	Varie	Brésil, Canada, France, Allemagne, Italie, Espagne, Royaume-Uni, États-Unis

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Clé privée selon la norme de cryptographie à clé publique (PKCS)	Informations d'identification	PKCS	Non	N'importe quel compte
Clé privée PuTTY	Informations d'identification	PUTTY_PRIVATE_KEY	Non	N'importe quel compte
Numéro d'assurance sociale (SIN)	Informations personnelles : PII	CANADA_SOCIAL_INSURANCE_NUMBER	Oui	Canada
Numéro de sécurité sociale (SSN)	Informations personnelles : PII	Selon le pays ou la région :SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER	Oui	Espagne, États-Unis
the section called "Clé d'API Stripe"	Informations d'identification	STRIPE_CREDENTIALS	Non	N'importe quel compte

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Numéro d'identification ou de référence du contribuable	Informations personnelles : PII	Selon le pays ou la région : AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER	Oui	Australie, Brésil, France, Allemagne, Inde, Italie, Espagne, Royaume-Uni, États-Unis
Identifiant unique de l'appareil (UDI)	Informations personnelles : PHI	MEDICAL_DEVICE_UDI	Oui	ETATS-UNIS

Type de données sensibles	Catégorie de données sensibles	ID d'identifiant de données géré	Mot-clé requis	Pays et régions
Numéro d'identification du véhicule (VIN)	Informations personnelles : PII	VEHICLE_IDENTIFICATION_NUMBER	Oui	N'importe lequel, si le VIN se trouve à proximité d'un mot clé dans l'une des langues suivantes : anglais, français, allemand, lituanien, polonais, portugais, roumain ou espagnol

Identifiants de données gérés pour les données d'identification

Amazon Macie peut détecter plusieurs types de données d'identification sensibles à l'aide d'identifiants de données gérés. Les rubriques de cette page spécifient chaque type et fournissent des informations sur l'identifiant de données géré conçu pour détecter les données. Chaque rubrique fournit les informations suivantes :

- ID d'identifiant de données gérées — Spécifie l'identifiant unique (ID) de l'identifiant de données gérées conçu pour détecter les données. Lorsque vous créez une tâche de découverte de données sensibles ou que vous configurez des paramètres de découverte automatique de données sensibles, vous pouvez utiliser cet ID pour indiquer si vous souhaitez que Macie utilise l'identifiant des données gérées lorsqu'il analyse les données.

- Pays et régions pris en charge : indique pour quels pays ou régions l'identifiant de données gérées applicable est conçu. Si l'identifiant des données gérées n'est pas conçu pour un pays ou une région en particulier, cette valeur est Any.
- Mot-clé obligatoire — Spécifie si la détection nécessite qu'un mot clé se trouve à proximité des données. Si un mot clé est requis, la rubrique fournit également des exemples de mots clés obligatoires. Pour plus d'informations sur la façon dont Macie utilise les mots clés lorsqu'il analyse les données, consultezExigences relatives aux mots-clés.
- Commentaires — Fournit tous les détails pertinents susceptibles d'affecter votre choix d'identifiant de données gérées ou votre enquête sur les cas signalés de données sensibles. Les détails incluent des informations telles que les normes prises en charge, les exigences de syntaxe et les exceptions.

Les rubriques sont répertoriées par ordre alphabétique par type de données sensibles.

Types de données sensibles

- Clé d'accès secrète AWS
- Clé d'API Google Cloud
- En-tête d'autorisation HTTP Basic
- Jeton Web JSON (JWT)
- Clé privée OpenSSH
- Clé privée PGP
- Clé privée selon la norme de cryptographie à clé publique (PKCS)
- Clé privée PuTTY
- Clé d'API Stripe

Clé d'accès secrète AWS

ID de l'identifiant des données gérées : AWS_CREDENTIALS

Pays et régions pris en charge : Tous

Mot-clé requis : Oui Les mots clés incluent : aws_secret_access_key, credentials, secret access key, secret key, set-awscredential

Commentaires : Macie ne signale pas les occurrences des séquences de caractères suivantes, qui sont couramment utilisées comme exemples fictifs : et. `je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY` `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

Clé d'API Google Cloud

ID de l'identifiant des données gérées : GCP_API_KEY

Pays et régions pris en charge : Tous

Mot-clé requis : Oui Les mots clés incluent : G_PLACES_KEY, GCP api key, GCP key, google cloud key, google-api-key, google-cloud-apikeys, GOOGLEKEY, X-goog-api-key

Commentaires : Macie ne peut détecter que le composant string (`keyString`) d'une clé d'API Google Cloud. Support n'inclut pas la détection de l'identifiant ou du nom d'affichage du composant d'une clé d'API Google Cloud.

En-tête d'autorisation HTTP Basic

ID de l'identifiant des données gérées : HTTP_BASIC_AUTH_HEADER

Pays et régions pris en charge : Tous

Mot-clé requis : Non

Commentaires : La détection nécessite un en-tête complet, y compris le nom du champ et la directive du schéma d'authentification, comme spécifié par la RFC 7617. Par exemple : `Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==` et `Proxy-Authorization: Basic dGVzdDoxMjPCow==`.

Jeton Web JSON (JWT)

ID de l'identifiant des données gérées : JSON_WEB_TOKEN

Pays et régions pris en charge : Tous

Mot-clé requis : Non

Commentaires : Macie peut détecter les jetons Web JSON (JWT) conformes aux exigences spécifiées par la RFC 7519 pour les structures de signature Web JSON (JWS). Les jetons peuvent être signés ou non.

Clé privée OpenSSH

ID de l'identifiant des données gérées : OPENSSH_PRIVATE_KEY

Pays et régions pris en charge : Tous

Mot-clé requis : Non

Commentaires : Aucun

Clé privée PGP

ID de l'identifiant des données gérées : PGP_PRIVATE_KEY

Pays et régions pris en charge : Tous

Mot-clé requis : Non

Commentaires : Aucun

Clé privée selon la norme de cryptographie à clé publique (PKCS)

ID de l'identifiant des données gérées : PKCS

Pays et régions pris en charge : Tous

Mot-clé requis : Non

Commentaires : Aucun

Clé privée PuTTY

ID de l'identifiant des données gérées : PUTTY_PRIVATE_KEY

Pays et régions pris en charge : Tous

Mot-clé requis : Non

Commentaires : Macie peut détecter les clés privées PuTTY qui utilisent les en-têtes et séquences d'en-têtes standard suivants `PuTTY-User-Key-File` :`Encryption`,,, `Comment`Public-Lines, `Private-Lines` et. `Private-MAC` Les valeurs d'en-tête peuvent contenir des caractères alphanumériques, des tirets (`-`) et des caractères de nouvelle ligne (ou). `\n` `\r` `Public-Lines`et `Private-Lines` les valeurs peuvent également contenir des barres obliques (`/`), des signes plus (+) et des signes égaux (=). `Private-MAC`les valeurs peuvent également contenir des signes plus

(+). Support n'inclut pas la détection des clés privées dont les valeurs d'en-tête contiennent d'autres caractères, tels que des espaces ou des traits de soulignement (_). Support n'inclut pas non plus la détection des clés privées qui incluent des en-têtes personnalisés.

Clé d'API Stripe

ID de l'identifiant des données gérées : STRIPE_CREDENTIALS

Pays et régions pris en charge : Tous

Mot-clé requis : Non

Commentaires : Macie ne signale pas les occurrences des séquences de caractères suivantes, qui sont couramment utilisées dans les exemples de code Stripe : `sk_test_4eC39HqLyjWDarjtT1zdp7dc` et`pk_test_TYooMQauvdEDq54NiTphI7jx`.

Identifiants de données gérés pour les informations financières

Amazon Macie peut détecter plusieurs types d'informations financières sensibles à l'aide d'identifiants de données gérés. Les rubriques de cette page répertorient chaque type et fournissent des informations sur les identificateurs de données gérés conçus pour détecter les données. Chaque rubrique fournit les informations suivantes :

- ID d'identifiant de données gérées — Spécifie l'identifiant unique (ID) pour un ou plusieurs identifiants de données gérées conçus pour détecter les données. Lorsque vous créez une tâche de découverte de données sensibles ou que vous configurez des paramètres de découverte automatique de données sensibles, vous pouvez utiliser ces identifiants pour spécifier les identifiants de données gérées que vous souhaitez que Macie utilise lors de l'analyse des données.
- Pays et régions pris en charge : indique pour quels pays ou régions les identifiants de données gérées applicables sont conçus. Si les identifiants de données gérés ne sont pas conçus pour des pays ou des régions spécifiques, cette valeur est Any.
- Mot-clé obligatoire — Spécifie si la détection nécessite qu'un mot clé se trouve à proximité des données. Si un mot clé est requis, la rubrique fournit également des exemples de mots clés obligatoires. Pour plus d'informations sur la façon dont Macie utilise les mots clés lorsqu'il analyse les données, consultezExigences relatives aux mots-clés.
- Commentaires — Fournit tous les détails pertinents susceptibles d'affecter votre choix d'identifiant de données gérées ou votre enquête sur les cas signalés de données sensibles. Les détails incluent des informations telles que les normes prises en charge, les exigences de syntaxe et les exceptions.

Les rubriques sont répertoriées par ordre alphabétique par type de données sensibles.

Types de données sensibles

- Numéro de compte bancaire
- Numéro de compte bancaire de base (BBAN)
- Date d'expiration de carte de crédit
- Données relatives à la bande magnétique des cartes de crédit
- Numéro de carte de crédit
- Code de vérification de carte de crédit
- Numéro de compte bancaire international (IBAN)

Numéro de compte bancaire

Macie peut détecter les numéros de comptes bancaires canadiens et américains composés de séquences de 9 à 17 chiffres et ne contenant aucun espace.

ID de l'identifiant des données gérées : BANK_ACCOUNT_NUMBER

Pays et régions pris en charge : Canada, États-Unis

Mot-clé requis : Oui Les mots clés incluent : bank account, bank acct, checking account, checking acct, deposit account, deposit acct, savings account, savings acct, chequing account, chequing acct

Commentaires : Cet identifiant de données gérées est explicitement conçu pour détecter les numéros de comptes bancaires au Canada et aux États-Unis. Ces pays n'utilisent pas les formats de numéro de compte bancaire de base (BBAN) ou de numéro de compte bancaire international (IBAN) définis par la norme internationale ISO pour la numérotation des comptes bancaires, comme spécifié par la norme ISO 13616. Pour détecter les numéros de comptes bancaires d'autres pays et régions, utilisez les identifiants de données gérés conçus pour ces formats. Pour plus d'informations, consultez Numéro de compte bancaire de base (BBAN) et Numéro de compte bancaire international (IBAN).

Numéro de compte bancaire de base (BBAN)

Macie peut détecter les numéros de compte bancaire de base (BBAN) conformes à la structure BBAN définie par la norme internationale ISO pour la numérotation des comptes bancaires, telle que spécifiée par la norme ISO 13616. Cela inclut les BBAN qui ne contiennent pas d'espaces ou qui utilisent des séparateurs d'espaces ou de tirets, par exemple, et. `NWBK60161331926819` `NWBK 6016 1331 9268 19` `NWBK-6016-1331-9268-19`

ID d'identifiant des données gérées : selon le pays ou la région, FRANCE_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER

Pays et régions pris en charge : France, Allemagne, Italie, Espagne, Royaume-Uni

Mot-clé requis : Oui Le tableau suivant répertorie les mots clés que Macie reconnaît pour des pays et des régions spécifiques.

Pays ou région	Mots clés
France	account code, account number, accountno#, accountnumber#, bban, code bancaire, compte bancaire, customer account id, customer account number, customer bank account id, iban, numéro de compte
Allemagne	account code, account number, accountno #, accountnumber#, bankleitzahl, bban, customer account id, customer account number, customer bank account id, geheimzahl, iban, kartennummer, kontonummer, kreditkartennummer, sepa
Italie	account code, account number, accountno #, accountnumber#, bban, codice bancario, conto bancario, customer account id, customer account number, customer bank account id, iban, numero di conto
Espagne	account code, account number, accountno #, accountnumber#, bban, código cuenta, código cuenta bancaria, cuenta cliente id, customer account ID, customer account number, customer bank account id, iban, número cuenta bancaria cliente, número cuenta cliente

Pays ou région	Mots clés
Royaume-Uni	account code, account number, accountno #, accountnumber#, bban, customer account id, customer account number, customer bank account id, iban, sepa

Commentaires : Ces identifiants de données gérés peuvent également détecter les numéros de compte bancaire internationaux (IBAN) conformes à la norme ISO 13616. Pour plus d'informations, consultez Numéro de compte bancaire international (IBAN). L'identifiant de données géré pour le Royaume-Uni (UK_BANK_ACCOUNT_NUMBER) peut également détecter les numéros de comptes bancaires nationaux pour le Royaume-Uni, par exemple,. `60-16-13 31926819`

Date d'expiration de carte de crédit

ID de l'identifiant des données gérées : CREDIT_CARD_EXPIRATION

Pays et régions pris en charge : Tous

Mot-clé requis : Oui Les mots clés incluent : exp d, exp m, exp y, expiration, expiry

Commentaires : Le support inclut la plupart des formats de date, tels que tous les chiffres, les combinaisons de chiffres et les noms des mois. Les composants de date peuvent être séparés par des barres obliques (/), des traits d'union (-) ou des mots clés applicables. Par exemple, Macie peut détecter des dates telles que`02/26`,`02/2026`, `Feb 202626-Feb`, et`expY=2026, expM=02`.

Données relatives à la bande magnétique des cartes de crédit

ID de l'identifiant des données gérées : CREDIT_CARD_MAGNETIC_STRIPE

Pays et régions pris en charge : Tous

Mot-clé requis : Oui Les mots clés incluent : card data, iso7813, mag, magstripe, stripe, swipe

Commentaires : Le support inclut les pistes 1 et 2.

Numéro de carte de crédit

ID d'identification des données gérées : CREDIT_CARD_NUMBER pour les numéros de carte de crédit situés à proximité d'un mot clé, CREDIT_CARD_NUMBER_(NO_KEYWORD) pour les numéros de carte de crédit qui ne sont pas à proximité d'un mot clé

Pays et régions pris en charge : Tous

Mot-clé requis : Variable. Les mots clés sont requis par l'identifiant des données CREDIT_CARD_NUMBER gérées. Les mots clés incluent : account number, american express, amex, bank card, c card, card, cc #, ccn, check card, cred card, credit, credit card, credit cards, credit no, credit num, dankort, debit, debit card, debit no, debit num, diners club, discover, electron, japanese card bureau, jcb, mastercard, mc, pan, payment account number, payment card number, pcn, pmnt #, pmnt card, pmnt no, pmnt number, union pay, visa. Les mots clés ne sont pas requis par l'identifiant des données CREDIT_CARD_NUMBER_(NO_KEYWORD) gérées.

Commentaires : La détection nécessite que les données soient une séquence de 13 à 19 chiffres conforme à la formule de vérification de Luhn et utilise un préfixe de numéro de carte standard pour les types de cartes de crédit suivants : American Express, Dankort, Diner's Club, Discover, Electron, Japanese Card Bureau (JCB), Mastercard et Visa. UnionPay

Macie ne signale pas les occurrences des séquences suivantes, que les émetteurs de cartes de crédit ont réservées aux tests publics : `122000000000003` `222240534324887722229909052570 51,2223007648726984,,2223577120017656,305693090259045200828282828210` `5204230080000017` `5204740009900014,5420923878724339,5454545454545454,5455330760000018,550690049000043` et`76009244561`.

Code de vérification de carte de crédit

ID de l'identifiant des données gérées : CREDIT_CARD_SECURITY_CODE

Pays et régions pris en charge : Tous

Mot-clé requis : Oui Les mots clés incluent : card id, card identification code, card identification number, card security code, card validation code, card validation number, card verification data, card verification value, cvc, cvc2, cvv, cvv2, elo verification code

Commentaires : Aucun

Numéro de compte bancaire international (IBAN)

Macie peut détecter les numéros de compte bancaire internationaux (IBAN) composés d'un maximum de 34 caractères alphanumériques, y compris des éléments tels que le code du pays. Plus précisément, Macie peut détecter les IBAN conformes à la norme internationale ISO pour la numérotation des comptes bancaires, telle que spécifiée par la norme ISO 13616. Cela inclut

les IBAN qui ne contiennent pas d'espaces ou qui utilisent des séparateurs d'espaces ou de tirets, par exemple, et. `GB29NWBK60161331926819` `GB29 NWBK 6016 1331 9268 19` `GB29-NWBK-6016-1331-9268-19` La détection inclut des contrôles de validation basés sur le schéma Modulus 97.

Identifiant des données gérées : selon le pays ou la région ALBANIA_BANK_ACCOUNT_NUMBER, ANDORRA_BANK_ACCOUNT_NUMBER, BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER, BRAZIL_BANK_ACCOUNT_NUMBER, BULGARIA_BANK_ACCOUNT_NUMBER, COSTA_RICA_BANK_ACCOUNT_NUMBER, CROATIA_BANK_ACCOUNT_NUMBER, CYPRUS_BANK_ACCOUNT_NUMBER, CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER, DENMARK_BANK_ACCOUNT_NUMBER, DOMINICAN_REPUBLIC_BANK_ACCOUNT_NUMBER, EGYPT_BANK_ACCOUNT_NUMBER, ESTONIA_BANK_ACCOUNT_NUMBER, FAROE_ISLANDS_BANK_ACCOUNT_NUMBER, FINLAND_BANK_ACCOUNT_NUMBER, FRANCE_BANK_ACCOUNT_NUMBER, GEORGIA_BANK_ACCOUNT_NUMBER, GERMANY_BANK_ACCOUNT_NUMBER, GREECE_BANK_ACCOUNT_NUMBER, GREENLAND_BANK_ACCOUNT_NUMBER, HUNGARY_BANK_ACCOUNT_NUMBER, ICELAND_BANK_ACCOUNT_NUMBER, IRELAND_BANK_ACCOUNT_NUMBER, ITALY_BANK_ACCOUNT_NUMBER, JORDAN_BANK_ACCOUNT_NUMBER, KOSOVO_BANK_ACCOUNT_NUMBER, LIECHTENSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER, MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_NUMBER, NETHERLANDS_BANK_ACCOUNT_NUMBER, NORTH_MACEDONIA_BANK_ACCOUNT_NUMBER, POLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER, SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER (pour les îles Vierges britanniques)

Pays et régions pris en charge : Albanie, Andorre, Bosnie-Herzégovine, Brésil, Bulgarie, Costa Rica, Croatie, Chypre, République tchèque, Danemark, République dominicaine, Égypte, Estonie, îles

Féroé, Finlande, France, Géorgie, Allemagne, Grèce, Groenland, Hongrie, Islande, Irlande, Italie, Jordanie, Kosovo, Liechtenstein, Lituanie, Malte, Mauritanie, Maurice, Monaco, Monténégro, Pays-Bas, Macédoine du Nord, Pologne, Portugal, Saint-Marin, Sénégal, Serbie, Slovaquie, Slovénie, Espagne, Suède, Suisse, Timor-Leste, Tunisie, Turquie, Royaume-Uni, Ukraine, Émirats arabes unis Emirates, îles Vierges britanniques

Mot-clé requis : Non

Commentaires : Les identifiants de données gérés pour la France, l'Allemagne, l'Italie, l'Espagne et le Royaume-Uni peuvent également détecter les numéros de compte bancaire de base (BBAN) conformes à la structure BBAN définie par la norme ISO 13616, si la séquence de caractères se trouve à proximité d'un mot clé. Pour plus d'informations, voir Numéro de compte bancaire de base (BBAN).

Identifiants de données gérés pour les informations de santé personnelles (PHI)

Amazon Macie peut détecter plusieurs types d'informations médicales personnelles (PHI) sensibles à l'aide d'identifiants de données gérés. Les rubriques de cette page spécifient chaque type et fournissent des informations sur l'identifiant de données géré conçu pour détecter les données. Chaque rubrique fournit les informations suivantes :

- ID d'identifiant de données gérées — Spécifie l'identifiant unique (ID) de l'identifiant de données gérées conçu pour détecter les données. Lorsque vous créez une tâche de découverte de données sensibles ou que vous configurez des paramètres de découverte automatique de données sensibles, vous pouvez utiliser cet ID pour indiquer si vous souhaitez que Macie utilise l'identifiant des données gérées lorsqu'il analyse les données.
- Pays et régions pris en charge : indique pour quels pays ou régions l'identifiant de données gérées applicable est conçu. Si l'identifiant des données gérées n'est pas conçu pour un pays ou une région en particulier, cette valeur est Any.
- Mot-clé obligatoire — Spécifie si la détection nécessite qu'un mot clé se trouve à proximité des données. Si un mot clé est requis, la rubrique fournit également des exemples de mots clés obligatoires. Pour plus d'informations sur la façon dont Macie utilise les mots clés lorsqu'il analyse les données, consultezExigences relatives aux mots-clés.
- Commentaires — Fournit tous les détails pertinents susceptibles d'affecter votre choix d'identifiant de données gérées ou votre enquête sur les cas signalés de données sensibles. Les détails incluent des informations telles que les normes prises en charge, les exigences de syntaxe et les exceptions.

Les rubriques sont répertoriées par ordre alphabétique par type de données sensibles.

Types de données sensibles

Numéro d'enregistrement de la Drug Enforcement Agency (DEA)

ID d'identifiant des données gérées : US_DRUG_ENFORCEMENT_AGENCY_NUMBER

Pays et régions pris en charge : États-Unis

Mot-clé requis : Oui. Les mots clés incluent : dea number, dea registration

Commentaires : Aucun

Numéro de réclamation d'assurance maladie (HICN)

ID d'identifiant des données gérées : USA_HEALTH_INSURANCE_CLAIM_NUMBER

Pays et régions pris en charge : États-Unis

Mot-clé requis : Oui. Les mots clés incluent : health insurance claim number, hic no, hic no., hic number, hic#, hicn, hicn#., hicno#

Commentaires : Aucun

Numéro d'assurance maladie ou d'identification médicale

Support inclus les numéros de carte européenne d'assurance maladie pour l'UE et la Finlande, les numéros d'assurance maladie pour la France, les identifiants des bénéficiaires de Medicare pour les États-Unis, les numéros du NHS pour le Royaume-Uni et les numéros de santé personnels pour le Canada.

ID d'identifiant des données gérées : selon le pays ou la région, CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER,

FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER

Pays et régions pris en charge : Canada, UE, Finlande, France, Royaume-Uni, États-Unis

Mot-clé requis : Oui. Le tableau suivant répertorie les mots clés que Macie reconnaît pour des pays et des régions spécifiques.

Pays ou région	Mots clés
Canada	canada healthcare number, msp number, personal healthcare number, phn, soins de santé
UE	assicurazione sanitaria numero, carta assicurazione numero, carte d'assurance maladie, carte européenne d'assurance maladie, ceam, ehic, ehic#, finlandehicnumber#, gesundheitskarte, hälsokort, health card, health card number, health insurance card, health insurance number, insurance card number, krankenversicherungskarte, krankenversicherungsnummer, medical account number, numero conto medico, numéro d'assurance maladie, numéro de carte d'assurance, numéro de compte medical, número de cuenta médica, número de seguro de salud, número de tarjeta de seguro, sairaanhoitokortin, sairausva kuutuskortti, sairausvakuutusnumero, sjukförsäkring nummer, sjukförsäkringskort, suomi ehic-numero, tarjeta de salud, terveyskortti, tessera sanitaria assicurazione numero, versicherungsnummer
Finlande	ehic, ehic#, finland health insurance card, finlandehicnumber#, finska sjukförsäkringskort, hälsokort, health card, health card number,

Pays ou région	Mots clés
	health insurance card, health insurance number, sairaanhoitokortin, sairaanhoitokortin , sairausvakuutuskortti, sairausvakuutusnum ero, sjukförsäkring nummer, sjukförsäkringskor t, suomen sairausvakuutuskortti, suomi ehic-numero, terveyskortti
France	carte d'assuré social, carte vitale, insurance card
Royaume-Uni	national health service, NHS
ETATS-UNIS	mbi, medicare beneficiary

Commentaires : Aucun

Code du système de codage des procédures communes pour les soins de santé (HCPCS)

ID d'identifiant des données gérées : USA_HEALTHCARE_PROCEDURE_CODE

Pays et régions pris en charge : États-Unis

Mot-clé requis : Oui. Les mots clés incluent : current procedural terminology, hcpcs, healthcare common procedure coding system

Commentaires : Aucun

Code national des médicaments (NDC)

ID d'identifiant des données gérées : USA_NATIONAL_DRUG_CODE

Pays et régions pris en charge : États-Unis

Mot-clé requis : Oui. Les mots clés incluent : national drug code, ndc

Commentaires : Aucun

Identifiant national du fournisseur (NPI)

ID d'identifiant des données gérées : USA_NATIONAL_PROVIDER_IDENTIFIER

Pays et régions pris en charge : États-Unis

Mot-clé requis : Oui. Les mots clés incluent : hipaa, n.p.i, national provider, npi

Commentaires : Aucun

Identifiant unique de l'appareil (UDI)

ID d'identifiant des données gérées : MEDICAL_DEVICE_UDI

Pays et régions pris en charge : États-Unis

Mot-clé requis : Oui. Les mots clés incluent : blood, blood bag, dev id, device id, device identifier, gs1, hibcc, iccbba, med, udi, unique device id, unique device identifier

Commentaires : Macie peut détecter les identifiants uniques des appareils (UDI) conformes aux formats approuvés par la Food and Drug Administration des États-Unis. Cela inclut les formats standard définis par GS1, HIBCC et ICCBBA. Le support de l'ICCBA concerne la norme ISBT.

Identifiants de données gérés pour les informations personnelles identifiables (PII)

Amazon Macie peut détecter plusieurs types d'informations personnelles sensibles (PII) à l'aide d'identifiants de données gérés. Les rubriques de cette page répertorient chaque type et fournissent des informations sur les identificateurs de données gérés conçus pour détecter les données. Chaque rubrique fournit les informations suivantes :

- ID d'identifiant de données gérées — Spécifie l'identifiant unique (ID) pour un ou plusieurs identifiants de données gérées conçus pour détecter les données. Lorsque vous créez une tâche de découverte de données sensibles ou que vous configurez des paramètres de découverte automatique de données sensibles, vous pouvez utiliser ces identifiants pour spécifier les identifiants de données gérées que vous souhaitez que Macie utilise lors de l'analyse des données.
- Pays et régions pris en charge : indique pour quels pays ou régions les identifiants de données gérées applicables sont conçus. Si les identifiants de données gérés ne sont pas conçus pour des pays ou des régions spécifiques, cette valeur est Any.
- Mot-clé obligatoire — Spécifie si la détection nécessite qu'un mot clé se trouve à proximité des données. Si un mot clé est requis, la rubrique fournit également des exemples de mots clés obligatoires. Pour plus d'informations sur la façon dont Macie utilise les mots clés lorsqu'il analyse les données, consultezExigences relatives aux mots-clés.
- Commentaires — Fournit tous les détails pertinents susceptibles d'affecter votre choix d'identifiant de données gérées ou votre enquête sur les cas signalés de données sensibles. Les détails

incluent des informations telles que les normes prises en charge, les exigences de syntaxe et les exceptions.

Les rubriques sont répertoriées par ordre alphabétique par type de données sensibles.

Types de données sensibles

- Date de naissance
- Numéro d'identification du permis de conduire
- Numéro de liste électorale
- Nom complet
- Coordonnées du système de positionnement global (GPS)
- Cookie HTTP
- Adresse postale
- Numéro d'identification nationale
- Numéro d'assurance nationale (NINO)
- Numéro de passeport
- Numéro de résidence permanente
- Phone number (Numéro de téléphone)
- Numéro d'assurance sociale (SIN)
- Numéro de sécurité sociale (SSN)
- Numéro d'identification ou de référence du contribuable
- Numéro d'identification du véhicule (VIN)

Date de naissance

ID de l'identifiant des données gérées : DATE_OF_BIRTH

Pays et régions pris en charge : Tous

Mot-clé requis : Oui. Les mots clés incluent : bday, b-day, birth date, birthday, date of birth, dob

Commentaires : Le support inclut la plupart des formats de date, tels que tous les chiffres, les combinaisons de chiffres et les noms des mois. Les composants de date peuvent être séparés par des espaces, des barres obliques (/) ou des traits d'union (-).

Numéro d'identification du permis de conduire

ID d'identifiant des données gérées : selon le pays ou la région, AUSTRALIA_DRIVERS_LICENSE, AUSTRIA_DRIVERS_LICENSE, BELGIUM_DRIVERS_LICENSE, BULGARIA_DRIVERS_LICENSE, CANADA_DRIVERS_LICENSE, CROATIA_DRIVERS_LICENSE, CYPRUS_DRIVERS_LICENSE, CZECHIA_DRIVERS_LICENSE, DENMARK_DRIVERS_LICENSE, DRIVERS_LICENSE (for the US), ESTONIA_DRIVERS_LICENSE, FINLAND_DRIVERS_LICENSE, FRANCE_DRIVERS_LICENSE, GERMANY_DRIVERS_LICENSE, GREECE_DRIVERS_LICENSE, HUNGARY_DRIVERS_LICENSE, INDIA_DRIVERS_LICENSE, IRELAND_DRIVERS_LICENSE, ITALY_DRIVERS_LICENSE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE

Pays et régions pris en charge : Australie, Autriche, Belgique, Bulgarie, Canada, Croatie, Chypre, République tchèque, Danemark, Estonie, Finlande, France, Allemagne, Grèce, Hongrie, Inde, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, Roumanie, Slovaquie, Slovénie, Espagne, Suède, Royaume-Uni, États-Unis

Mot-clé requis : Oui. Le tableau suivant répertorie les mots clés que Macie reconnaît pour des pays et des régions spécifiques.

Pays ou région	Mots clés
Australie	dl#, dl:, dlno#, driver licence, driver license, driver permit, drivers lic., drivers licence, driver's licence, drivers license, driver's license, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit
Autriche	führerschein, fuhrerschein, führerschein republik österreich, fuhrerschein republik osterreich
Belgique	fuehrerschein, fuehrerschein- nr, fuehrersc heinnummer, fuhrerschein, führerschein,

Pays ou région	Mots clés
	fuhrerschein- nr, führerschein- nr, fuhrersch einnummer, führerscheinnummer, numéro permis conduire, permis de conduire, rijbewijs, rijbewijsnummer
Bulgarie	превозно средство, свидетелство за управление на моторно, свидетелство за управление на мпс, сумпс, шофьорска книжка
Canada	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit, permis de conduire
Croatie	vozačka dozvola
Chypre	άδεια οδήγησης
République tchèque	číslo licence, číslo licence řidiče, číslo řidičskéh o průkazu, ovladače lic., povolení k jízdě, povolení řidiče, řidiči povolení, řidičský prúkaz, řidičský průkaz
Danemark	kørekort, kørekortnummer
Estonie	juhi litsentsi number, juhiloa number, juhiluba, juhiluba number
Finlande	ajokortin numero, ajokortti, förare lic., körkort, körkort nummer, kuljettaja lic., permis de conduire

Pays ou région	Mots clés
France	permis de conduire
Allemagne	fuehrerschein, fuehrerschein- nr, fuehrersc heinnummer, fuhrerschein, führerschein, fuhrerschein- nr, führerschein- nr, fuhrersch einnummer, führerscheinnummer
Grèce	δεια οδήγησης, adeia odigisis
Hongrie	illesztőprogramok lic, jogosítvány, jogsi, licencszám, vezető engedély, vezetői engedély
Inde	driver licence, driver licences, driver license, driver licenses, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, driving licence, driving license
Irlande	ceadúnas tiomána
Italie	patente di guida, patente di guida numero, patente guida, patente guida numero
Lettonie	autovadītāja apliecība, licences numurs, vadītāja apliecība, vadītāja apliecības numurs, vadītāja atļauja, vadītāja licences numurs, vadītāji lic.
Lituanie	vairuotojo pažymėjimas
Luxembourg	fahrerlaubnis, führerschäin
Malte	liċenzja tas-sewqan
Pays-Bas	permis de conduire, rijbewijs, rijbewijsnummer

Pays ou région	Mots clés
Pologne	numer licencyjny, prawo jazdy, zezwolenie na prowadzenie
Portugal	carta de condução, carteira de habilitação, carteira de motorist, carteira habilitação, carteira motorist, licença condução, licença de condução, número de licença, número licença, permissão condução, permissão de condução
Roumanie	numărul permisului de conducere, permis de conducere
Slovaquie	číslo licencie, číslo vodičského preukazu, ovládače lic., povolenia vodičov, povolenie jazdu, povolenie na jazdu, povolenie vodiča, vodičský preukaz
Slovénie	vozniško dovoljenje
Espagne	carnet conducer, el carnet de conducer, licencia conducer, licencia de manejo, número carnet conducer, número de carnet de conducer, número de permiso conducer, número de permiso de conducer, número licencia conducer, número permiso conducer, permiso conducción, permiso conducer, permiso de conducción
Suède	ajokortin numero, dlno# ajokortti, drivere lic., förare lic., körkort, körkort nummer, körkortsn ummer, kuljettajat lic.

Pays ou région	Mots clés
Royaume-Uni	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit
ETATS-UNIS	dl#, dl:, dlno#, driver licence, driver licences, driver license, driver licenses, driver permit, drivers lic., drivers licence, driver's licence, drivers licences, driver's licences, drivers license, driver's license, drivers licenses, driver's licenses, drivers permit, driver's permit, drivers permit number, driving licence, driving license, driving permit

Commentaires : Aucun

Numéro de liste électorale

ID de l'identifiant des données gérées : UK_ELECTORAL_ROLL_NUMBER

Pays et régions pris en charge : Royaume-Uni

Mot-clé requis : Oui. Les mots clés incluent : electoral #, electoral number, electoral roll #, electoral roll no., electoral roll number, electoralrollno

Commentaires : Aucun

Nom complet

ID de l'identifiant des données gérées : NAME

Pays et régions pris en charge : Tous

Mot-clé requis : Non

Commentaires : Macie ne peut détecter que les noms complets. Le support est limité aux jeux de caractères latins.

Coordonnées du système de positionnement global (GPS)

ID de l'identifiant des données gérées : LATITUDE_LONGITUDE

Pays et régions pris en charge : Tous, si les coordonnées se trouvent à proximité d'un mot clé anglais.

Mot-clé requis : Oui. Les mots clés incluent : coordinate, coordinates, lat long, latitude longitude, position

Commentaires : Macie peut détecter les coordonnées GPS si les coordonnées de latitude et de longitude sont stockées par paire et qu'elles sont au format décimal (DD), par exemple. `41.948614,-87.655311` Support n'inclut pas la détection de coordonnées au format : degrés décimaux minutes (DDM), par exemple `41°56.9168'N 87°39.3187'W` ; ou au format degrés, minutes, secondes (DMS), par exemple. `41°56'55.0104"N 87°39'19.1196"W`

Cookie HTTP

ID de l'identifiant des données gérées : HTTP_COOKIE

Pays et régions pris en charge : Tous

Mot-clé requis : Non

Commentaires : La détection nécessite un nom complet `Cookie` ou un `Set-Cookie` en-tête. L'en-tête peut inclure une ou plusieurs paires nom-valeur, par exemple : `Set-Cookie: id=TWlrZQ` et. `Cookie: session=3948; lang=en`

Adresse postale

Identifiant des données gérées : ADDRESS (pour l'Australie, le Canada, la France, l'Allemagne, l'Italie, l'Espagne, le Royaume-Uni et les États-Unis), BRAZIL_CEP_CODE (pour le Código de Endereçamento Postal du Brésil)

Pays et régions pris en charge : Australie, Brésil, Canada, France, Allemagne, Italie, Espagne, Royaume-Uni, États-Unis

Mot-clé requis : Variable. Les mots clés ne sont pas requis par l'identifiant des données ADDRESS gérées. Les mots clés sont requis par l'identifiant des données BRAZIL_CEP_CODE gérées. Les

mots clés incluent : cep, código de endereçamento postal, codigo de endereçamento postal, código postal, codigo postal

Commentaires : Bien qu'aucun mot clé ne soit requis pour l'identifiant des données ADDRESS gérées, la détection nécessite une adresse incluant le nom d'une ville ou d'un lieu et le code postal ou postal correspondant dans un pays ou une région pris en charge. L'identifiant de données BRAZIL_CEP_CODE géré ne peut détecter que la partie Código de Endereçamento Postal (CEP) d'une adresse.

Numéro d'identification nationale

Support inclus les numéros Aadhaar pour l'Inde, les numéros Codice Fiscale pour l'Italie, les identifiants Documento Nacional de Identidad (DNI) pour l'Espagne, les codes de l'Institut national français des statistiques et des études économiques (INSEE), les numéros de carte nationale d'identité allemande et les numéros du Registro Geral (RG) pour le Brésil.

ID d'identifiant des données gérées : selon le pays ou la région, BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, INDIA_AADHAAR_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER

Pays et régions pris en charge : Brésil, France, Allemagne, Inde, Italie, Espagne

Mot-clé requis : Oui. Le tableau suivant répertorie les mots clés que Macie reconnaît pour des pays et des régions spécifiques.

Pays ou région	Mots clés
Brésil	registro geral, rg
France	assurance sociale, carte nationale d'identit é, cni, code sécurité sociale, French social security number, fssn#, insee, insurance number, national id number, nationalid#, numéro d'assurance, sécurité sociale, sécurité sociale non., sécurité sociale numéro, social, social security, social security number, socialsecuritynumber, ss#, ssn, ssn#

Pays ou région	Mots clés
Allemagne	ausweisnummer, id number, identification number, identity number, insurance number, personal id, personalausweis
Inde	aadhaar, aadhar, adhaar, uidai
Italie	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
Espagne	dni, dni#, dninúmero#, documento nacional de identidad, identidad único, identidadúnico#, insurance number, national identification number, national identity, nationalid#, nationali dno#, número nacional identidad, personal identification number, personal identity no, unique identity number, uniqueid#

Commentaires : Aucun

Numéro d'assurance nationale (NINO)

ID de l'identifiant des données gérées : UK_NATIONAL_INSURANCE_NUMBER

Pays et régions pris en charge : Royaume-Uni

Mot-clé requis : Oui. Les mots clés incluent : insurance no., insurance number, insurance#, national insurance number, nationalinsurance#, nationalinsurancenumber, nin, nino

Commentaires : Aucun

Numéro de passeport

ID d'identifiant des données gérées : selon le pays ou la région, CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER

Pays et régions pris en charge : Canada, France, Allemagne, Italie, Espagne, Royaume-Uni, États-Unis

Mot-clé requis : Oui. Le tableau suivant répertorie les mots clés que Macie reconnaît pour des pays et des régions spécifiques.

Pays ou région	Mots clés
Canada	passeport, passeport#, passport, passport#, passportno, passportno#
France	numéro de passeport, passeport, passeport #, passeport n °, passeport non
Allemagne	ausstellungsdatum, ausstellungsort, geburtsdatum, passport, passports, reisepass, reisepass–nr, reisepassnummer
Italie	italian passport number, numéro passeport , numéro passeport italien, passaporto, passaporto italiana, passaporto numero, passport number, repubblica italiana passaporto
Espagne	españa pasaporte, libreta pasaporte, número pasaporte, pasaporte, passport, passport book, passport no, passport number, spain passport
Royaume-Uni	passeport #, passeport n °, passeport non, passeportn °, passport #, passport no, passport number, passport#, passportid
ETATS-UNIS	passport, travel document

Commentaires : Aucun

Numéro de résidence permanente

ID de l'identifiant des données gérées : CANADA_NATIONAL_IDENTIFICATION_NUMBER

Pays et régions pris en charge : Canada

Mot-clé requis : Oui. Les mots clés incluent : carte résident permanent, numéro carte résident permanent, numéro résident permanent, permanent resident card, permanent resident card number, permanent resident no, permanent resident no., permanent resident number, pr no, pr no., pr non, pr number, résident permanent no., résident permanent non

Commentaires : Aucun

Phone number (Numéro de téléphone)

ID d'identifiant des données gérées : selon le pays ou la région, BRAZIL_PHONE_NUMBER, FRANCE_PHONE_NUMBER, GERMANY_PHONE_NUMBER, ITALY_PHONE_NUMBER, PHONE_NUMBER (for Canada and the US), SPAIN_PHONE_NUMBER, UK_PHONE_NUMBER

Pays et régions pris en charge : Brésil, Canada, France, Allemagne, Italie, Espagne, Royaume-Uni, États-Unis

Mot-clé requis : Variable. Si un mot clé se trouve à proximité des données, il n'est pas nécessaire que le numéro inclue un code de pays. Les mots clés incluent : cell, contact, fax, fax number, mobile, phone, phone number, tel, telephone, telephone number. Pour le Brésil, les mots clés incluent également : cel, celular, fone, móvel, número residencial, numero residencial, telefone. Si un mot clé ne se trouve pas à proximité des données, il est nécessaire que le numéro inclue un code de pays.

Commentaires : Pour les États-Unis, l'assistance inclut les numéros gratuits.

Numéro d'assurance sociale (SIN)

ID de l'identifiant des données gérées : CANADA_SOCIAL_INSURANCE_NUMBER

Pays et régions pris en charge : Canada

Mot-clé requis : Oui. Les mots clés incluent : canadian id, numéro d'assurance sociale, sin, social insurance number

Commentaires : Aucun

Numéro de sécurité sociale (SSN)

ID d'identifiant des données gérées : selon le pays ou la régionSPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER

Pays et régions pris en charge : Espagne, États-Unis

Mot-clé requis : Oui. Pour l'Espagne, les mots clés incluent : número de la seguridad social, social security no., social security number, socialsecurityno#, ssn, ssn#. Pour les États-Unis, les mots clés incluent : social security, ss#, ssn.

Commentaires : Aucun

Numéro d'identification ou de référence du contribuable

Support inclus : numéros CIF, NIE et NIF pour l'Espagne ; numéros CNPJ et CPF pour le Brésil ; numéros Codice Fiscale pour l'Italie ; ITins pour les États-Unis ; PAN pour l'Inde ; numéros Steueridentifikationsnummer pour l'Allemagne ; TFN pour l'Australie ; TIN pour la France ; et numéros TRN et UTR pour le Royaume-Uni.

ID d'identifiant des données gérées : selon le pays ou la région, AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

Pays et régions pris en charge : Australie, Brésil, France, Allemagne, Inde, Italie, Espagne, Royaume-Uni, États-Unis

Mot-clé requis : Oui. Le tableau suivant répertorie les mots clés que Macie reconnaît pour des pays et des régions spécifiques.

Pays ou région	Mots clés
Australie	tax file number, tfn
Brésil	cadastro de pessoa física, cadastro de pessoa fisica, cadastro de pessoas físicas, cadastro de pessoas fisicas, cadastro nacional da pessoa jurídica, cadastro nacional da pessoa juridica, cnpj, cpf
France	numéro d'identification fiscal, tax id, tax identific ation number, tax number, tin, tin#

Pays ou région	Mots clés
Allemagne	identifikationsnummer, steuer id, steueride ntifikationsnummer, steuernummer, tax id, tax identification number, tax number
Inde	e-pan, pan card, pan number, permanent account number
Italie	codice fiscal, dati anagrafici, ehic, health card, health insurance card, p. iva, partita i.v.a., personal data, tax code, tessera sanitaria
Espagne	cif, cif número, cifnúmero#, nie, nif, número de contribuyente, número de identidad de extranjero, número de identificación fiscal, número de impuesto corporativo, personal tax number, tax id, tax identification number, tax number, tin, tin#
Royaume-Uni	paye, tax id, tax id no., tax id number, tax identification, tax identification#, tax no., tax number, tax reference, tax#, taxid#, temporary reference number, tin, trn, unique tax reference, unique taxpayer reference, utr
ETATS-UNIS	i.t.i.n., numéro d'identification individuel du contribuable, itin

Commentaires : Aucun

Numéro d'identification du véhicule (VIN)

ID de l'identifiant des données gérées : VEHICLE_IDENTIFICATION_NUMBER

Pays et régions pris en charge : Tous, si le VIN se trouve à proximité d'un mot clé dans l'une des langues suivantes : anglais, français, allemand, lituanien, polonais, portugais, roumain ou espagnol.

Mot-clé requis : Oui. Les mots clés incluent : Fahrgestellnummer, niv, numarul de identificare, numarul seriei de sasiu, numer VIN, Número de Identificação do Veículo, Número de Identificación de Automóviles, numéro d'identification du véhicule, vehicle identification number, vin, VIN numeris

Commentaires : Macie peut détecter les VIN composés d'une séquence de 17 caractères et respecter les normes ISO 3779 et 3780. Ces normes ont été conçues pour être utilisées dans le monde entier.

Création d'identifiants de données personnalisés dans Amazon Macie

UNidentifiant de données personnaliséest un ensemble de critères que vous définissez pour détecter les données sensibles dans les objets Amazon Simple Storage Service (Amazon S3). Les critères sont constitués d'une expression régulière (regex) qui définit un modèle de texte à mettre en correspondance et, éventuellement, des séquences de caractères et une règle de proximité qui affinent les résultats.

Les identifiants de données personnalisés vous permettent de définir des critères de détection qui reflètent les scénarios particuliers de votre entreprise, la propriété intellectuelle ou les données propriétaires, par exemple les identifiants des employés, les numéros de compte client ou les classifications de données internes. Si vous configureztâches de découverte de données sensiblesoudécouverte automatique de données sensiblespour utiliser ces identifiants, vous pouvez analyser les objets S3 d'une manière qui complèteidentifiants de données gérésqu'Amazon Macie fournit.

Outre les critères de détection, vous pouvez définir des paramètres de gravité personnalisés pour les résultats de données sensibles produits par un identifiant de données personnalisé. Par défaut, Macie attribue leMoyensévérité de tous les résultats produits par un identifiant de données personnalisé : la gravité ne change pas en fonction du nombre d'occurrences de texte correspondant aux critères de détection d'un identifiant de données personnalisé. En définissant des paramètres de gravité personnalisés, vous pouvez spécifier la gravité à attribuer en fonction du nombre d'occurrences de texte correspondant aux critères.

Rubriques

- Définition de critères de détection pour les identificateurs de données personnalisés
- Définition des paramètres de gravité de la recherche pour les identificateurs de données personnalisés

- Création d'identifiants de données personnalisés
- Support de Regex dans les identifiants de données personnalisés

Définition de critères de détection pour les identificateurs de données personnalisés

Lorsque vous créez un identifiant de données personnalisé, vous spécifiez une expression régulière (regex) qui définit un modèle de texte à faire correspondre aux objets S3. Macie prend en charge un sous-ensemble de la syntaxe du modèle regex fourni parBibliothèque d'expressions régulières compatibles avec Perl (PCRE). Pour plus d'informations, voirSupport Regexplus loin dans cette section.

Vous pouvez également spécifier des séquences de caractères, telles que des mots et des phrases, ainsi qu'une règle de proximité pour affiner les résultats.

Mots clés

Il s'agit de séquences de caractères spécifiques qui doivent se trouver à proximité d'un texte correspondant au modèle d'expression régulière. Les exigences de proximité varient en fonction du format de stockage ou du type de fichier d'un objet S3 :

- Pour les données structurées en colonnes, Macie inclut un résultat si le texte correspond au modèle d'expression régulière et si un mot clé figure dans le nom du champ ou de la colonne qui stocke le texte, ou si le texte est précédé d'un mot clé dans le même champ ou la même valeur de cellule et si la distance de correspondance maximale par rapport à celui-ci se trouve dans la même zone. Cela est vrai pour les classeurs Microsoft Excel, les fichiers CSV et les fichiers TSV.
- Pour les données structurées basées sur des enregistrements, Macie inclut un résultat si le texte correspond au modèle d'expression régulière et s'il se trouve dans la distance de correspondance maximale d'un mot clé. Le mot clé peut figurer dans le nom d'un élément du chemin d'accès au champ ou au tableau qui stocke le texte, ou il peut précéder le champ ou le tableau qui stocke le texte et faire partie de la même valeur dans celui-ci. Cela est vrai pour les conteneurs d'objets Apache Avro, les fichiers Apache Parquet, les fichiers JSON et les fichiers JSON Lines.
- Pour les données non structurées, Macie inclut un résultat si le texte correspond au modèle d'expression régulière et s'il est précédé d'un mot clé et se trouve dans les limites de la distance de correspondance maximale par rapport à celui-ci. Cela est vrai pour les fichiers Adobe

Portable Document Format, les documents Microsoft Word, les messages électroniques et les fichiers texte non binaires autres que les fichiers CSV, JSON, JSON Lines et TSV. Cela inclut toutes les données structurées, telles que les tables, présentes dans ces types de fichiers.

Vous pouvez spécifier jusqu'à 50 mots-clés. Chaque mot clé peut contenir de 3 à 90 caractères UTF-8. Les mots-clés ne sont pas sensibles à la casse.

Distance de correspondance maximale

Il s'agit d'une règle de proximité basée sur les caractères pour les mots clés. Macie utilise ce paramètre pour déterminer si un mot clé précède le texte qui correspond au modèle d'expression régulière. Le paramètre définit le nombre maximum de caractères pouvant exister entre la fin d'un mot clé complet et la fin du texte correspondant au modèle de regex. Si le texte correspond au modèle de regex, apparaît après au moins un mot-clé complet et se trouve dans la distance spécifiée par rapport au mot-clé, Macie l'inclut dans les résultats. Sinon, Macie l'exclut des résultats.

Vous pouvez spécifier une distance comprise entre 1 et 300 caractères. La distance par défaut est de 50 caractères. Pour de meilleurs résultats, cette distance doit être supérieure au nombre minimum de caractères de texte que la regex est conçue pour détecter. Si seule une partie du texte se trouve dans la distance de correspondance maximale d'un mot clé, Macie ne l'inclut pas dans les résultats.

Ignorer les mots

Il s'agit de séquences de caractères spécifiques à exclure des résultats. Si le texte correspond au modèle d'expression régulière mais qu'il contient un mot à ignorer, Macie ne l'inclut pas dans les résultats.

Vous pouvez spécifier jusqu'à 10 mots à ignorer. Chaque mot à ignorer peut contenir de 4 à 90 caractères UTF-8. Les mots ignorés sont sensibles à la casse.

Par exemple, de nombreuses entreprises ont une syntaxe spécifique pour les ID d'employés. L'une de ces syntaxes peut être la suivante : une majuscule indiquant si l'employé travaille à temps plein (F) ou à temps partiel (P), suivi d'un trait d'union (-), suivi d'une séquence de huit chiffres identifiant l'employé. Les exemples sont les suivants :F-12345678, pour un salarié à temps plein, etP-87654321, pour un salarié à temps partiel.

Si vous créez un identificateur de données personnalisé pour détecter les ID d'employé qui utilisent cette syntaxe, vous pouvez utiliser l'expression regex suivante : `[A-Z]-\d{8}`. Pour affiner l'analyse

et éviter les faux positifs, vous pouvez également configurer l'identifiant de données personnalisé pour utiliser les mots-clésemployéetidentifiant de l'employéet une distance de correspondance maximale de 20 caractères. Avec ces critères, les résultats incluent du texte qui correspond à l'expression régulière uniquement si le texte apparaît après le mot cléemployéouidentifiant de l'employéet tout le texte se trouve à moins de 20 caractères de l'un de ces mots-clés.

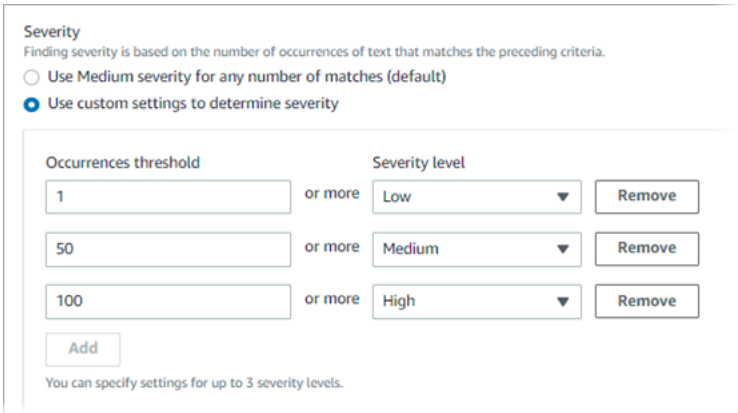
Pour découvrir comment les mots clés peuvent vous aider à trouver des données sensibles et à éviter les faux positifs, regardez la vidéo suivante :Comment Amazon Macie utilise des mots clés pour découvrir des données sensibles.

Définition des paramètres de gravité de la recherche pour les identificateurs de données personnalisés

Lorsque vous créez un identifiant de données personnalisé, vous pouvez également définir des paramètres de gravité personnalisés pour les résultats de données sensibles produits par l'identifiant. Par défaut, Macie attribue leMoyengravité de tous les résultats produits par un identifiant de données personnalisé : si un objet S3 contient au moins une occurrence de texte qui correspond aux critères de détection d'un identifiant de données personnalisé, Macie attribue automatiquementMoyengravité de la constatation qui en résulte.

Les paramètres de gravité personnalisés vous permettent de spécifier le niveau de gravité à attribuer en fonction du nombre d'occurrences de texte correspondant aux critères de détection de l'identifiant de données personnalisé. Pour ce faire, vous définissezseuils d'occurrencepour un maximum de trois niveaux de gravité :Faible(moins sévère),Moyen, etÉlevé(le plus grave). Unseuil d'occurrencesest le nombre minimum de correspondances qui doivent exister dans un objet S3 pour produire un résultat présentant la gravité spécifiée. Si vous spécifiez plusieurs seuils, les seuils doivent être classés par ordre croissant de gravité, en commençant parFaiblepourÉlevé.

Par exemple, l'image suivante montre les paramètres de gravité d'un identifiant de données personnalisé qui spécifie trois seuils d'occurrence, un pour chaque niveau de gravité pris en charge par Macie.



Le tableau suivant indique la gravité des résultats produits par l'identifiant de données personnalisé.

Seuil d'occurrences	Niveau de gravité	Résultat
1	Faible	Si un objet S3 contient de 1 à 49 occurrences de texte qui correspondent aux critères de détection, la gravité du résultat obtenu estFaible.
50	Medium	Si un objet S3 contient entre 50 et 99 occurrences de texte qui correspondent aux critères de détection, la gravité du résultat obtenu estMoyen.
100	Élevée	Si un objet S3 contient au moins 100 occurrences de texte qui correspondent aux critères de détection, la gravité de la découverte obtenue estÉlevé.

Vous pouvez également utiliser les paramètres de gravité pour spécifier si vous souhaitez créer une constatation. Si un objet S3 contient moins d'occurrences que le seuil d'occurrences le plus bas, Macie ne crée pas de résultat.

Création d'identifiants de données personnalisés

Suivez ces étapes pour créer un identifiant de données personnalisé à l'aide de la console Amazon Macie. Pour créer un identifiant de données personnalisé par programmation, utilisezCreateCustomDataIdentifierfonctionnement de l'API Amazon Macie.

Pour créer un identificateur de données personnalisé

1. Ouvrez la console Amazon Macie à l'adressehttps://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, sous Settings (Paramètres), choisissez Custom data identifiers (Identificateurs de données personnalisés).
3. Sélectionnez Create (Créer).
4. Dans la zone Nom, saisissez un nom pour l'identificateur de données personnalisé. Le nom peut contenir jusqu'à 128 caractères.

   Évitez d'inclure des données sensibles dans le nom. D'autres utilisateurs de votre compte peuvent peut-être voir le nom, selon les actions qu'ils sont autorisés à effectuer dans Macie.
5. (Facultatif) PourDescriptif, entrez une brève description de l'identifiant de données personnalisé. La description peut contenir jusqu'à 512 caractères.

   Évitez d'inclure des données sensibles dans la description. Les autres utilisateurs de votre compte pourront peut-être voir la description, selon les actions qu'ils sont autorisés à effectuer dans Macie.
6. PourExpression régulière, entrez l'expression régulière (regex) qui définit le modèle de texte correspondant. La regex peut contenir jusqu'à 512 caractères. Pour en savoir plus sur la syntaxe et les contraintes prises en charge, voirSupport Regexplus loin dans cette section.
7. (Facultatif) PourMots clés, entrez jusqu'à 50 séquences de caractères (séparées par des virgules) pour définir un texte spécifique qui doit se trouver à proximité du texte correspondant au modèle de regex. Chaque mot clé peut contenir de 3 à 90 caractères UTF-8. Les mots-clés ne sont pas sensibles à la casse.

   Macie inclut une occurrence dans les résultats uniquement si le texte correspond au modèle d'expression régulière et si le texte se trouve dans la distance de correspondance maximale de l'un de ces mots-clés, comme expliqué danssujet précédent.
8. (Facultatif) PourIgnorer les mots, entrez jusqu'à 10 séquences de caractères (séparées par des virgules) qui définissent le texte spécifique à exclure des résultats. Chaque mot à ignorer peut contenir de 4 à 90 caractères UTF-8. Les mots ignorés sont sensibles à la casse.

Macie exclut une occurrence des résultats si le texte correspond au modèle d'expression régulière mais qu'il contient l'un de ces mots d'ignorance.

9. (Facultatif) PourDistance de correspondance maximale, entrez le nombre maximum de caractères pouvant exister entre la fin d'un mot-clé et la fin du texte correspondant au modèle de regex. La distance peut être comprise entre 1 et 300 caractères. La distance par défaut est de 50 caractères.

   Macie inclut une occurrence dans les résultats uniquement si le texte correspond au modèle d'expression régulière et si le texte se trouve à moins de cette distance d'un mot clé complet, comme expliqué danssujet précédent.

10. PourGravité, choisissez la manière dont vous souhaitez que Macie attribue la gravité aux résultats de données sensibles produits par l'identifiant de données personnalisé :

    - Pour attribuer automatiquement leMoyengravité de tous les résultats, choisissezUtiliser le niveau de gravité moyen pour n'importe quel nombre de correspondances (par défaut). Avec cette option, Macie attribue automatiquement leMoyengravité d'une découverte si l'objet S3 concerné contient une ou plusieurs occurrences de texte qui correspondent aux critères de détection.
    - Pour attribuer la gravité en fonction des seuils d'occurrence que vous spécifiez, choisissezUtiliser des paramètres personnalisés pour déterminer la gravité. Ensuite, utilisez leSeuil d'occurrencesetNiveau de gravitéoptions permettant de spécifier le nombre minimum de correspondances qui doivent exister dans un objet S3 pour produire une constatation avec une gravité sélectionnée.

      Par exemple, pour attribuer leÉlevégravité d'une constatation signalant 100 occurrences ou plus de texte correspondant aux critères de détection, entrez**`100`**dans leSeuil d'occurrencesboîte puis choisissezÉlevéà partir duNiveau de gravitéliste.

      Vous pouvez spécifier jusqu'à trois seuils d'occurrence, un pour chaque niveau de gravité pris en charge par Macie :Faible(pour les moins graves),Moyen, ouÉlevé(pour les plus sévères). Si vous en spécifiez plusieurs, les seuils doivent être classés par ordre croissant de gravité, en commençant parFaiblepourÉlevé. Si un objet S3 contient moins d'occurrences que le seuil le plus bas spécifié, Macie ne crée pas de résultat.

11. (Facultatif) PourÉtiquettes, choisissezAjouter un tag, puis entrez jusqu'à 50 balises à attribuer à l'identifiant de données personnalisé.

UNétiquetteest une étiquette que vous définissez et attribuez à certains types deAWSressources. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Les balises peuvent vous aider à identifier, classer et gérer les ressources de différentes manières, par exemple en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Pour en savoir plus, consultez Marquage des ressources Amazon Macie.

12. (Facultatif) PourÉvaluer, entrez jusqu'à 1 000 caractères dansExemples de donnéesboîte, puis choisissezTestpour tester les critères de détection. Macie évalue les données de l'échantillon et indique le nombre d'occurrences de texte correspondant aux critères. Vous pouvez répéter cette étape autant de fois que vous le souhaitez pour affiner et optimiser les critères.

> **Note**
>
> Nous vous recommandons vivement de tester et d'affiner les critères de détection avant d'enregistrer l'identifiant de données personnalisé. Les identificateurs de données personnalisés étant utilisés par les tâches de découverte de données sensibles, vous ne pouvez pas modifier un identifiant de données personnalisé après l'avoir enregistré. Cela vous permet de disposer d'un historique immuable des découvertes et des résultats de découverte de données sensibles pour les audits ou les enquêtes que vous réalisez en matière de confidentialité et de protection des données.

13. Lorsque vous avez terminé, choisissez Submit (Soumettre).

Macie teste les paramètres et vérifie qu'elle peut compiler la regex. En cas de problème avec l'un des paramètres ou la regex, une erreur se produit et indique la nature du problème. Une fois les problèmes résolus, vous pouvez enregistrer l'identifiant de données personnalisé.

Support de Regex dans les identifiants de données personnalisés

Macie prend en charge un sous-ensemble de la syntaxe du modèle regex fourni parBibliothèque d'expressions régulières compatibles avec Perl (PCRE). Parmi les constructions fournies par la bibliothèque PCRE, Macie ne prend pas en charge les éléments de modèle suivants :

- Références rétrospectives
- Capture de groupes
- Modèles conditionnels

- Code intégré
- Indicateurs de modèles globaux, tels que`/i`,`/m`, et`/x`
- Modèles récursifs
- Assertions positives et négatives à largeur nulle, rétrospectives et prospectives, telles que`?=`,`?!`,`?<=`, et`?<!`

Pour créer des modèles de regex efficaces pour les identifiants de données personnalisés, tenez également compte des conseils et recommandations suivants :

- Ancrages— Utilisez des ancres (^ou$) uniquement si vous vous attendez à ce que le modèle apparaisse au début ou à la fin d'un fichier, et non au début ou à la fin d'une ligne.
- Répétitions bornées— Pour des raisons de performance, Macie limite la taille des groupes de répétitions bornés. Par exemple,`\d{100,1000}`ne compilera pas dans Macie. Pour approximer cette fonctionnalité, vous pouvez utiliser une répétition ouverte telle que`\d{100,}`.
- Insensibilité aux majuscules— Pour rendre certaines parties d'un motif insensibles aux majuscules, vous pouvez utiliser le`(?i)`construire au lieu de`/i`drapeau.
- Rendement— Il n'est pas nécessaire d'optimiser les préfixes ou les alternances manuellement. Par exemple, modifier`/hello|hi|hey/`pour`/h(?:ello|i|ey)/`n'améliorera pas les performances.
- Wildcards— Pour des raisons de performances, Macie limite le nombre de caractères génériques répétés. Par exemple,`a*b*a*`ne compilera pas dans Macie.

Pour se protéger contre les expressions mal formées ou de longue durée, Macie teste automatiquement les modèles d'expressions régulières par rapport à une collection d'exemples de texte.

Définition des exceptions relatives aux données sensibles à l'aide des listes d'autorisation Amazon Macie

Les listes d'autorisation d'Amazon Macie vous permettent de définir un texte et des modèles de texte que Macie doit ignorer lorsqu'elle inspecte les objets d'Amazon Simple Storage Service (Amazon S3), vous pouvez définir un texte et des modèles de texte que Macie doit ignorer lorsqu'elle inspecte les objets de la recherche de données sensibles. Il s'agit généralement d'exceptions relatives aux données sensibles pour vos scénarios ou votre environnement particuliers. Si les données correspondent à un texte ou à un modèle de texte dans une liste d'autorisation, Macie ne signale pas

les données, même si les données correspondent aux critères d'un identifiant de données géré ou d'un identifiant de données personnalisé. En utilisant des listes d'autorisation, vous pouvez affiner votre analyse des données Amazon S3 et réduire le bruit.

Vous pouvez créer et utiliser deux types de listes d'autorisation dans Macie :

- Texte prédéfini : pour ce type de liste, vous devez spécifier certaines séquences de caractères à ignorer, par exemple les noms des représentants publics de votre organisation, des numéros de téléphone spécifiques ou des exemples de données spécifiques que votre organisation utilise pour les tests. Si vous utilisez ce type de liste, Macie ignore le texte qui correspond exactement à une entrée de la liste.

  Ce type de liste d'autorisation est utile si vous souhaitez spécifier des mots, des phrases et d'autres types de séquences de caractères qui ne sont pas sensibles, qui ne sont pas susceptibles de changer et qui ne respectent pas nécessairement un modèle commun.
- Expression régulière : pour ce type de liste, vous spécifiez une expression régulière (regex) qui définit un modèle de texte à ignorer, par exemple, les numéros de téléphone publics de votre organisation, les adresses e-mail du domaine de votre organisation ou des exemples de données structurées que votre organisation utilise à des fins de test. Si vous utilisez ce type de liste, Macie ignore le texte qui correspond entièrement au modèle défini par la liste.

  Ce type de liste d'autorisation est utile si vous souhaitez spécifier un texte qui n'est pas sensible, mais qui varie ou est susceptible de changer, tout en respectant un modèle commun.

Après avoir créé une liste d'autorisation, vous pouvez créer et configurer des tâches de découverte de données sensibles pour l'utiliser, ou l'ajouter à vos paramètres de découverte automatique de données sensibles. Macie utilise ensuite la liste lorsqu'elle analyse les données. Si Macie trouve du texte qui correspond à une entrée ou à un modèle dans une liste autorisée, Macie ne signale pas cette occurrence de texte dans les résultats de données sensibles, les statistiques et les autres types de résultats.

Vous pouvez créer et utiliser des listes d'autorisation dans toutes les Régions AWS où Macie est actuellement disponible, à l'exception de la région Asie-Pacifique (Osaka).

Rubriques

- Autoriser les options et les exigences relatives aux listes dans Amazon Macie
- Création et gestion de listes d'autorisations dans Amazon Macie

Autoriser les options et les exigences relatives aux listes dans Amazon Macie

Dans Amazon Macie, vous pouvez utiliser des listes d'autorisation pour spécifier du texte ou des modèles de texte que vous souhaitez que Macie ignore lorsqu'il inspecte des objets Amazon Simple Storage Service (Amazon S3) pour détecter la présence de données sensibles. Macie propose des options pour deux types de listes d'autorisation : du texte prédéfini et des expressions régulières.

Une liste de texte prédéfini est utile si vous souhaitez que Macie ignore des mots, des phrases ou d'autres types de séquences de caractères que vous ne considérez pas comme sensibles. Les noms des représentants publics de votre organisation, les numéros de téléphone spécifiques ou les exemples de données spécifiques que votre organisation utilise pour les tests en sont des exemples. Si Macie trouve du texte qui correspond aux critères d'un identifiant de données géré ou personnalisé et que le texte correspond également à une entrée d'une liste d'autorisation, Macie ne signale pas cette occurrence de texte dans les résultats relatifs aux données sensibles, les statistiques et les autres types de résultats.

Une expression régulière (regex) est utile si vous souhaitez que Macie ignore le texte qui varie ou est susceptible de changer tout en respectant un modèle commun. L'expression régulière indique un modèle de texte à ignorer. Il s'agit par exemple des numéros de téléphone publics de votre organisation, des adresses e-mail du domaine de votre organisation ou des exemples de données structurés que votre organisation utilise pour les tests. Si Macie trouve du texte qui correspond aux critères d'un identifiant de données géré ou personnalisé et que le texte correspond également à un modèle d'expression régulière dans une liste d'autorisation, Macie ne signale pas cette occurrence de texte dans les résultats de données sensibles, les statistiques et les autres types de résultats.

Vous pouvez créer et utiliser les deux types de listes d'autorisation dans tous les Régions AWS endroits où Macie est actuellement disponible, à l'exception de la région Asie-Pacifique (Osaka). Lorsque vous créez et gérez des listes d'autorisation, gardez à l'esprit les options et exigences suivantes. Notez également que les entrées de liste autorisées et les modèles de regex pour les adresses postales ne sont pas pris en charge.

Rubriques

Options et exigences relatives aux listes de texte prédéfini

Pour ce type de liste d'autorisation, vous fournissez un fichier texte en clair délimité par des lignes qui répertorie les séquences de caractères spécifiques à ignorer. Les entrées de liste sont généralement des mots, des phrases et d'autres types de séquences de caractères que vous ne considérez pas comme sensibles, qui ne sont pas susceptibles de changer et qui ne suivent pas nécessairement un schéma spécifique. Si vous utilisez ce type de liste, Amazon Macie ne signale pas les occurrences de texte correspondant exactement à une entrée de la liste. Macie traite chaque entrée de liste comme une valeur littérale de chaîne.

Pour utiliser ce type de liste d'autorisation, commencez par créer la liste dans un éditeur de texte et enregistrez-la sous forme de fichier texte brut. Téléchargez ensuite la liste dans un compartiment S3 à usage général. Assurez-vous également que les paramètres de stockage et de chiffrement du bucket et de l'objet permettent à Macie de récupérer et de déchiffrer la liste. Créez et configurez ensuite les paramètres de la liste dans Macie.

Après avoir configuré les paramètres dans Macie, nous vous recommandons de tester la liste d'autorisations avec un petit ensemble de données représentatif de votre compte ou de votre organisation. Pour tester une liste, vous pouvez créer une tâche unique et configurer la tâche pour qu'elle utilise la liste en plus des identifiants de données gérés et des identifiants de données personnalisés que vous utilisez généralement pour analyser les données. Vous pouvez ensuite consulter les résultats de la tâche : résultats de découverte de données sensibles, résultats de découverte de données sensibles, ou les deux. Si les résultats de la tâche ne correspondent pas à vos attentes, vous pouvez modifier et tester la liste jusqu'à ce que les résultats soient conformes à vos attentes.

Une fois que vous avez terminé de configurer et de tester une liste d'autorisations, vous pouvez créer et configurer des tâches supplémentaires pour l'utiliser, ou l'ajouter aux paramètres de découverte automatique des données sensibles de votre compte. Lorsque ces tâches commencent à s'exécuter ou que le cycle d'analyse de découverte automatique suivant démarre, Macie récupère la dernière version de la liste sur Amazon S3 et la stocke dans une mémoire temporaire. Macie utilise ensuite cette copie temporaire de la liste lorsqu'il inspecte les objets S3 à la recherche de données sensibles.

Lorsqu'une tâche est terminée ou que le cycle d'analyse est terminé, Macie supprime définitivement de la mémoire sa copie de la liste. La liste ne persiste pas dans Macie. Seuls les paramètres de la liste sont conservés dans Macie.

> **Important**
>
> Comme les listes de texte prédéfini ne sont pas conservées dans Macie, il est important de vérifier régulièrement l'état de vos listes d'autorisation. Si Macie ne parvient pas à récupérer ou à analyser une liste pour laquelle vous avez configuré une tâche ou une découverte automatique, Macie n'utilise pas la liste. Cela peut produire des résultats inattendus, tels que la découverte de données sensibles pour le texte que vous avez spécifié dans la liste.

Rubriques

- Exigences en matière de syntaxe
- Besoins de stockage
- Exigences en matière de chiffrement/déchiffrement
- Considérations et recommandations relatives à la conception

Exigences en matière de syntaxe

Lorsque vous créez ce type de liste d'autorisations, tenez compte des exigences suivantes concernant le fichier de la liste :

- La liste doit être stockée sous forme de fichier texte brut (`text/plain`), tel qu'un fichier .txt, .text ou .plain.
- La liste doit utiliser des sauts de ligne pour séparer les entrées individuelles. Par exemple :

```
Akua Mansa
John Doe
Martha Rivera
425-555-0100
425-555-0101
425-555-0102
```

Macie traite chaque ligne comme une entrée unique et distincte dans la liste. Le fichier peut également contenir des lignes vierges pour améliorer la lisibilité. Macie ignore les lignes vides lorsqu'il analyse le fichier.

- Chaque entrée peut contenir de 1 à 90 caractères UTF-8.
- Chaque entrée doit correspondre exactement et complètement au texte à ignorer. Macie ne prend pas en charge l'utilisation de caractères génériques ou de valeurs partielles pour les entrées. Macie traite chaque entrée comme une valeur littérale de chaîne. Les correspondances ne sont pas sensibles à la casse.
- Le fichier peut contenir de 1 à 100 000 entrées.
- La taille de stockage totale du fichier ne peut pas dépasser 35 Mo.

Besoins de stockage

Lorsque vous ajoutez et gérez des listes d'autorisations dans Amazon S3, tenez compte des exigences et recommandations de stockage suivantes :

- Support régional — Une liste d'autorisation doit être stockée dans un compartiment Région AWS identique à celui de votre compte Macie. Macie ne peut pas accéder à une liste d'autorisation si elle est stockée dans une autre région.
- Propriété du compartiment : une liste d'autorisation doit être stockée dans un compartiment qui vous appartient Compte AWS. Si vous souhaitez que d'autres comptes utilisent la même liste d'autorisations, pensez à créer une règle de réplication Amazon S3 pour répliquer la liste dans les compartiments appartenant à ces comptes. Pour plus d'informations sur la réplication d'objets S3, consultez la section Réplication d'objets dans le guide de l'utilisateur d'Amazon Simple Storage Service.

  En outre, votre identité AWS Identity and Access Management (IAM) doit disposer d'un accès en lecture au bucket et à l'objet qui stockent la liste. Sinon, vous ne serez pas autorisé à créer ou à mettre à jour les paramètres de la liste ou à vérifier son statut à l'aide de Macie.
- Types et classes de stockage : une liste d'autorisations doit être stockée dans un compartiment à usage général, et non dans un compartiment de répertoire. En outre, il doit être stocké à l'aide de l'une des classes de stockage suivantes : Reduced Redundancy (RRS), S3 Glacier Instant Retrieval, S3 Intelligent-Tiering, S3 One Zone-IA, S3 Standard ou S3 Standard-IA.
- Politiques de compartiment — Si vous stockez une liste d'autorisations dans un compartiment doté d'une politique de compartiment restrictive, assurez-vous que cette politique autorise Macie

à récupérer la liste. Pour ce faire, vous pouvez ajouter une condition pour le rôle lié au service Macie à la politique du bucket. Pour plus d'informations, consultez Autoriser Macie à accéder aux compartiments et aux objets S3.

Assurez-vous également que la politique autorise votre identité IAM à avoir un accès en lecture au bucket. Sinon, vous ne serez pas autorisé à créer ou à mettre à jour les paramètres de la liste ou à vérifier son statut à l'aide de Macie.

- Chemins d'objet : si vous stockez plusieurs listes d'autorisation dans Amazon S3, le chemin d'objet de chaque liste doit être unique. En d'autres termes, chaque liste d'autorisation doit être stockée séparément en tant qu'objet S3 distinct.
- Gestion des versions : lorsque vous ajoutez une liste d'autorisations à un bucket, nous vous recommandons d'activer également le versionnement pour le bucket. Vous pouvez ensuite utiliser des valeurs de date et d'heure pour corréler les versions de la liste avec les résultats des tâches de découverte de données sensibles et des cycles automatisés de découverte de données sensibles utilisant la liste. Cela peut vous aider dans le cadre des audits ou des enquêtes que vous effectuez en matière de confidentialité et de protection des données.
- Verrouillage des objets : pour empêcher la suppression ou le remplacement d'une liste d'autorisations pendant un certain temps ou indéfiniment, vous pouvez activer le verrouillage d'objet pour le compartiment qui stocke la liste. L'activation de ce paramètre n'empêche pas Macie d'accéder à la liste. Pour plus d'informations sur ce paramètre, consultez la section Utilisation de S3 Object Lock dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Exigences en matière de chiffrement/déchiffrement

Si vous chiffrez une liste d'autorisations dans Amazon S3, la politique d'autorisations pour le rôle lié au service Macie accorde généralement à Macie les autorisations dont il a besoin pour déchiffrer la liste. Cela dépend toutefois du type de chiffrement utilisé :

- Si une liste est chiffrée à l'aide d'un chiffrement côté serveur avec une clé gérée Amazon S3 (SSE-S3), Macie peut déchiffrer la liste. Le rôle lié à un service pour votre compte Macie accorde à Macie les autorisations dont il a besoin.
- Si une liste est chiffrée à l'aide d'un chiffrement côté serveur avec un système AWS géré AWS KMS key (DSSE-KMS ou SSE-KMS), Macie peut déchiffrer la liste. Le rôle lié à un service pour votre compte Macie accorde à Macie les autorisations dont il a besoin.
- Si une liste est chiffrée à l'aide d'un chiffrement côté serveur géré par le client AWS KMS key (DSSE-KMS ou SSE-KMS), Macie ne peut déchiffrer la liste que si vous autorisez Macie à utiliser

la clé. Pour savoir comment procéder, veuillez consulter Permettre à Macie d'utiliser un système géré par le client AWS KMS key.

> **Note**
>
> Vous pouvez chiffrer une liste contenant un client géré AWS KMS key dans un magasin de clés externe. Cependant, la clé peut alors être plus lente et moins fiable qu'une clé entièrement gérée en interne AWS KMS. Si un problème de latence ou de disponibilité empêche Macie de déchiffrer la liste, Macie n'utilise pas la liste lorsqu'il analyse les objets S3. Cela peut produire des résultats inattendus, tels que la découverte de données sensibles pour le texte que vous avez spécifié dans la liste. Pour réduire ce risque, pensez à stocker la liste dans un compartiment S3 configuré pour utiliser la clé comme clé de compartiment S3.
>
> Pour plus d'informations sur l'utilisation des clés KMS dans les magasins de clés externes, consultez la section Stockages de clés externes dans le manuel du AWS Key Management Service développeur. Pour plus d'informations sur l'utilisation des clés de compartiment S3, consultez la section Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

- Si une liste est chiffrée à l'aide d'un chiffrement côté serveur avec une clé fournie par le client (SSE-C) ou d'un chiffrement côté client, Macie ne peut pas déchiffrer la liste. Envisagez plutôt d'utiliser le chiffrement SSE-S3, DSSE-KMS ou SSE-KMS.

Si une liste est chiffrée à l'aide d'une clé KMS AWS gérée ou d'une clé KMS gérée par le client, votre identité AWS Identity and Access Management (IAM) doit également être autorisée à utiliser la clé. Sinon, vous ne serez pas autorisé à créer ou à mettre à jour les paramètres de la liste ou à vérifier son statut à l'aide de Macie. Pour savoir comment vérifier ou modifier les autorisations associées à une clé KMS, consultez la section Politiques relatives aux clés AWS KMS dans le guide du AWS Key Management Service développeur.

Pour obtenir des informations détaillées sur les options de chiffrement des données Amazon S3, consultez la section Protection des données par le chiffrement dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Considérations et recommandations relatives à la conception

En général, Macie traite chaque entrée d'une liste d'autorisation comme une valeur littérale de chaîne. C'est-à-dire que Macie ignore chaque occurrence de texte qui correspond exactement à une entrée complète dans une liste d'autorisation. Les correspondances ne sont pas sensibles à la casse.

Cependant, Macie utilise les entrées dans le cadre d'un cadre d'extraction et d'analyse de données plus large. Le framework inclut des fonctions d'apprentissage automatique et de correspondance de modèles qui prennent en compte des dimensions telles que les variations grammaticales et syntaxiques et, dans de nombreux cas, la proximité des mots clés. Le framework prend également en compte le type de fichier ou le format de stockage d'un objet S3. Par conséquent, gardez à l'esprit les considérations et recommandations suivantes lorsque vous ajoutez et gérez les entrées dans une liste d'autorisation.

Préparez-vous à différents types de fichiers et formats de stockage

Pour les données non structurées, telles que le texte d'un fichier Adobe Portable Document Format (.pdf), Macie ignore le texte qui correspond exactement à une entrée complète dans une liste d'autorisation, y compris le texte qui s'étend sur plusieurs lignes ou pages.

Pour les données structurées, telles que les données en colonnes dans un fichier CSV ou les données basées sur des enregistrements dans un fichier JSON, Macie ignore le texte qui correspond exactement à une entrée complète dans une liste d'autorisation si tout le texte est stocké dans un seul champ, cellule ou tableau. Cette exigence ne s'applique pas aux données structurées stockées dans un fichier par ailleurs non structuré, tel qu'un tableau dans un fichier .pdf.

Par exemple, considérez le contenu suivant dans un fichier CSV :

```
Name,Account ID
Akua Mansa,111111111111
John Doe,222222222222
```

Si `Akua Mansa` et `John Doe` sont des entrées dans une liste d'autorisation, Macie ignore ces noms dans le fichier CSV. Le texte complet de chaque entrée de liste est enregistré dans un seul `Name` champ.

À l'inverse, considérez un fichier CSV contenant les colonnes et les champs suivants :

```
First Name,Last Name,Account ID
```

```
Akua,Mansa,111111111111
John,Doe,222222222222
```

Si `Akua Mansa` et `John Doe` sont des entrées dans une liste autorisée, Macie n'ignore pas ces noms dans le fichier CSV. Aucun des champs du fichier CSV ne contient le texte complet d'une entrée dans la liste d'autorisation.

Inclure les variations courantes

Ajoutez des entrées pour les variations courantes de données numériques, de noms propres, de termes et de séquences de caractères alphanumériques. Par exemple, si vous ajoutez des noms ou des phrases contenant un seul espace entre les mots, ajoutez également des variantes qui incluent deux espaces entre les mots. De même, ajoutez des mots et des phrases contenant ou non des caractères spéciaux, et envisagez d'inclure des variations syntaxiques et sémantiques courantes.

Pour le numéro de téléphone américain 425-555-0100, par exemple, vous pouvez ajouter les entrées suivantes à une liste d'autorisation :

```
425-555-0100
425.555.0100
(425) 555-0100
+1-425-555-0100
```

Pour la date du 1er février 2022 dans un contexte multinational, vous pouvez ajouter des entrées qui incluent des variations syntaxiques courantes pour l'anglais et le français, y compris des variations qui incluent ou non des caractères spéciaux :

```
February 1, 2022
1 février 2022
1 fevrier 2022
Feb 01, 2022
1 fév 2022
1 fev 2022
02/01/2022
01/02/2022
```

Pour les noms de personnes, incluez des entrées correspondant aux différentes formes de nom que vous ne considérez pas comme sensibles. Par exemple, incluez : le prénom suivi du nom de famille ; le nom de famille suivi du prénom, le prénom et le nom de famille séparés par un espace ; le prénom et le nom de famille séparés par deux espaces ; et les surnoms.

Pour le nom Martha Rivera, par exemple, vous pouvez ajouter :

```
Martha Rivera
Martha  Rivera
Rivera, Martha
Rivera,  Martha
Rivera Martha
Rivera  Martha
```

Si vous souhaitez ignorer les variantes d'un nom spécifique contenant de nombreuses parties, créez une liste d'autorisation qui utilise plutôt une expression régulière. Par exemple, pour le nom Dr. Martha Lyda Rivera, PhD, vous pouvez utiliser l'expression régulière suivante : `^(Dr. )?Martha\s(Lyda|L\.)?\s?Rivera,?( PhD)?$`

Options et exigences relatives aux expressions régulières dans les listes d'autorisation

Pour ce type de liste d'autorisation, vous spécifiez une expression régulière (regex) qui définit un modèle de texte à ignorer, par exemple, les numéros de téléphone publics de votre organisation, les adresses e-mail du domaine de votre organisation ou des exemples de données structurés que votre organisation utilise pour les tests. L'expression régulière définit un modèle commun pour un type spécifique de données que vous ne considérez pas comme sensibles. Si vous utilisez ce type de liste d'autorisation, Amazon Macie ne signale pas les occurrences de texte qui correspondent parfaitement au modèle spécifié. Contrairement à une liste d'autorisation qui spécifie le texte prédéfini à ignorer, vous créez et stockez l'expression régulière et tous les autres paramètres de liste dans Macie.

Lorsque vous créez ou mettez à jour ce type de liste d'autorisation, vous pouvez tester l'expression régulière de la liste avec des exemples de données avant de l'enregistrer. Nous vous recommandons de le faire avec plusieurs ensembles d'échantillons de données. Si vous créez une expression régulière trop générale, Macie risque d'ignorer les occurrences de texte que vous considérez comme sensibles. Si une expression régulière est trop spécifique, Macie peut ne pas ignorer les occurrences de texte que vous ne considérez pas comme sensibles. Pour se protéger contre les expressions mal formées ou de longue durée, Macie compile et teste automatiquement l'expression régulière par rapport à un ensemble d'exemples de texte, et vous informe des problèmes à résoudre.

Pour des tests supplémentaires, nous vous recommandons de tester également l'expression régulière de la liste avec un petit ensemble de données représentatif de votre compte ou de votre organisation. Pour ce faire, vous pouvez créer une tâche unique et configurer la tâche pour utiliser la

liste en plus des identifiants de données gérés et des identifiants de données personnalisés que vous utilisez généralement pour analyser les données. Vous pouvez ensuite consulter les résultats de la tâche : résultats de découverte de données sensibles, résultats de découverte de données sensibles, ou les deux. Si les résultats de la tâche diffèrent de ce que vous attendez, vous pouvez modifier et tester l'expression régulière jusqu'à ce que les résultats soient ceux que vous attendez.

Après avoir configuré et testé une liste d'autorisations, vous pouvez créer et configurer des tâches supplémentaires pour l'utiliser, ou l'ajouter aux paramètres de découverte automatique des données sensibles de votre compte. Lorsque ces tâches sont exécutées ou que Macie effectue une découverte automatique pour votre compte, Macie utilise la dernière version de l'expression régulière de la liste pour analyser les données.

Rubriques

Support syntaxique et recommandations

Une liste d'autorisation peut spécifier une expression régulière (regex) contenant jusqu'à 512 caractères. Macie prend en charge un sous-ensemble de la syntaxe du modèle regex fournie par la bibliothèque Perl Compatible Regular Expressions (PCRE). Parmi les constructions fournies par la bibliothèque PCRE, Macie ne prend pas en charge les éléments de modèle suivants :

- Références rétrospectives
- Capture de groupes
- Modèles conditionnels
- Code intégré
- Indicateurs de modèles globaux, tels que `/i`/`m`, et `/x`
- Motifs récursifs
- Assertions de largeur zéro rétrospectives et prospectives positives et négatives, telles que,, et `?=` `?!` `?<=` `?<!`

Pour créer des modèles d'expression régulière efficaces pour les listes d'autorisation, tenez également compte des conseils et recommandations suivants :

- Ancrages : utilisez des ancres (^ou$) uniquement si vous vous attendez à ce que le motif apparaisse au début ou à la fin d'un fichier, et non au début ou à la fin d'une ligne.
- Répétitions bornées — Pour des raisons de performance, Macie limite la taille des groupes de répétitions bornés. Par exemple, `\d{100,1000}` ne compilera pas dans Macie. Pour utiliser approximativement cette fonctionnalité, vous pouvez utiliser une répétition ouverte telle que`\d{100,}`.
- Insensibilité majuscules/minuscules — Pour rendre certaines parties d'un modèle insensibles aux majuscules et minuscules, vous pouvez utiliser la `(?i)` construction au lieu du `/i` drapeau.
- Performances — Il n'est pas nécessaire d'optimiser manuellement les préfixes ou les alternances. Par exemple, le passage `/hello|hi|hey/` à `/h(?:ello|i|ey)/` n'améliorera pas les performances.
- Wildcards — Pour des raisons de performance, Macie limite le nombre de jokers répétés. Par exemple, `a*b*a*` ne compilera pas dans Macie.
- Alternance : pour spécifier plusieurs modèles dans une seule liste d'autorisation, vous pouvez utiliser l'opérateur d'alternance (`|`) pour concaténer les modèles. Dans ce cas, Macie utilise la logique OR pour combiner les motifs et former un nouveau modèle. Par exemple, si vous le spécifiez`(apple|orange)`, Macie reconnaît à la fois pomme et orange comme une correspondance et ignore les occurrences des deux mots. Si vous concaténez des modèles, veillez à limiter la longueur totale de l'expression concaténée à 512 caractères ou moins.

Enfin, lorsque vous développez l'expression régulière, concevez-la pour qu'elle s'adapte à différents types de fichiers et formats de stockage. Macie utilise le regex dans le cadre d'un cadre d'extraction et d'analyse de données plus large. Le framework prend en compte le type de fichier ou le format de stockage d'un objet S3. Pour les données structurées, telles que les données en colonnes dans un fichier CSV ou les données basées sur des enregistrements dans un fichier JSON, Macie ignore le texte qui correspond parfaitement au modèle uniquement si tout le texte est stocké dans un seul champ, cellule ou tableau. Cette exigence ne s'applique pas aux données structurées stockées dans un fichier par ailleurs non structuré, tel qu'un tableau dans un fichier Adobe Portable Document Format (.pdf). Pour les données non structurées, telles que le texte d'un fichier .pdf, Macie ignore le texte qui correspond parfaitement au modèle, y compris le texte qui s'étend sur plusieurs lignes ou pages.

Exemples

Les exemples suivants illustrent des modèles de regex valides pour certains scénarios courants.

Adresses e-mail

Si vous utilisez un identifiant de données personnalisé pour détecter les adresses e-mail, vous pouvez ignorer les adresses e-mail que vous ne considérez pas comme sensibles, telles que les adresses e-mail de votre organisation.

Pour ignorer les adresses e-mail d'un domaine de deuxième ou de premier niveau en particulier, vous pouvez utiliser ce modèle :

```
[a-zA-Z0-9_.+\\-]+@example\.com
```

Où *exemple* est le nom du domaine de deuxième niveau et *com* est le domaine de premier niveau. Dans ce cas, Macie fait correspondre et ignore les adresses telles que johndoe@example.com et john.doe@example.com.

Pour ignorer les adresses e-mail d'un domaine particulier dans un domaine générique de premier niveau (gTLD), tel que .com ou .gov, vous pouvez utiliser ce modèle :

```
[a-zA-Z0-9_.+\\-]+@example\.[a-zA-Z]{2,}
```

Par *exemple*, le nom du domaine. Dans ce cas, Macie fait correspondre et ignore les adresses telles que johndoe@example.com, john.doe@example.gov et johndoe@example.edu.

Pour ignorer les adresses e-mail d'un domaine particulier dans un domaine de premier niveau correspondant à un code de pays (ccTLD), tel que .ca pour le Canada ou .au pour l'Australie, vous pouvez utiliser ce modèle :

```
[a-zA-Z0-9_.+\\-]+@example\.(ca|au)
```

Par *exemple,* le nom du domaine et les ccTLD *ca* et *au* sont des ccTLD spécifiques à ignorer. Dans ce cas, Macie fait correspondre et ignore les adresses telles que johndoe@example.ca et john.doe@example.au.

Pour ignorer les adresses e-mail associées à un domaine et à un gTLD particuliers et inclure des domaines de troisième et quatrième niveaux, vous pouvez utiliser ce modèle :

```
[a-zA-Z0-9_.+\\-]+@([a-zA-Z0-9-]+\.)?[a-zA-Z0-9-]+\.example\.com
```

Où *exemple* est le nom du domaine et *com* est le gTLD. Dans ce cas, Macie fait correspondre et ignore les adresses telles que johndoe@www.example.com et john.doe@www.team.example.com.

Numéros de téléphone

Macie fournit des identifiants de données gérés qui peuvent détecter les numéros de téléphone de plusieurs pays et régions. Pour ignorer certains numéros de téléphone, tels que les numéros gratuits ou les numéros de téléphone publics de votre organisation, vous pouvez utiliser des modèles tels que les suivants.

Pour ignorer les numéros de téléphone américains gratuits qui utilisent l'indicatif régional 800 et qui sont au format (800) ###-#### :

```
^\(?800\)?[ -]?\d{3}[ -]?\d{4}$
```

Pour ignorer les numéros de téléphone américains gratuits qui utilisent l'indicatif régional 888 et qui sont au format (888) ###-#### :

```
^\(?888\)?[ -]?\d{3}[ -]?\d{4}$
```

Pour ignorer les numéros de téléphone français à 10 chiffres qui incluent le code de pays 33 et sont au format +33 ## ## ## ## ## :

```
^\+33 \d( \d\d){4}$
```

Pour ignorer les numéros de téléphone américains et canadiens qui utilisent des codes régionaux et de change particuliers, n'incluez pas de code de pays et sont formatés comme suit : (###) ###-#### :

```
^\(?123\)?[ -]?555[ -]?\d{4}$
```

Où *123* est le code régional et *555* est le code d'échange.

Pour ignorer les numéros de téléphone américains et canadiens qui utilisent des codes régionaux et d'échange particuliers, incluent un code de pays et sont formatés comme +1 (###) ###-#### :

```
^\+1\(?123\)?[ -]?555[ -]?\d{4}$
```

Où *123* est le code régional et *555* est le code d'échange.

Création et gestion de listes d'autorisations dans Amazon Macie

Dans Amazon Macie, une liste d'autorisation définit un texte spécifique ou un modèle de texte que vous souhaitez que Macie ignore lorsqu'il inspecte les objets Amazon Simple Storage Service (Amazon S3) à la recherche de données sensibles. Si le texte correspond à une entrée ou à un

modèle d'une liste d'autorisation, Macie ne le signale pas dans les résultats relatifs aux données sensibles, les statistiques ou les autres types de résultats, même s'il répond aux critères d'un identifiant de données géré ou d'un identifiant de données personnalisé.

Vous pouvez créer et gérer les types de listes d'autorisation suivants dans Macie.

Texte prédéfini

Utilisez ce type de liste pour spécifier des mots, des phrases et d'autres types de séquences de caractères qui ne sont pas sensibles, qui ne sont pas susceptibles de changer et qui ne suivent pas nécessairement un schéma commun. Les noms des représentants publics de votre organisation, les numéros de téléphone spécifiques et les exemples de données spécifiques que votre organisation utilise pour les tests en sont des exemples. Si vous utilisez ce type de liste, Macie ignore le texte qui correspond exactement à une entrée de la liste.

Pour ce type de liste, vous créez un fichier texte en clair délimité par des lignes qui répertorie le texte spécifique à ignorer. Vous stockez ensuite le fichier dans un compartiment S3 et configurez les paramètres permettant à Macie d'accéder à la liste contenue dans le compartiment. Vous pouvez ensuite créer et configurer des tâches de découverte de données sensibles pour utiliser la liste, ou ajouter la liste aux paramètres de découverte automatique de données sensibles de votre compte. Lorsque chaque tâche commence à s'exécuter ou que le cycle d'analyse de découverte automatique suivant démarre, Macie récupère la dernière version de la liste sur Amazon S3. Macie utilise ensuite cette version de la liste lorsqu'il inspecte les objets S3 à la recherche de données sensibles. Si Macie trouve du texte qui correspond exactement à une entrée de la liste, Macie ne signale pas cette occurrence de texte comme une donnée sensible.

Expression régulière

Utilisez ce type de liste pour spécifier une expression régulière (regex) qui définit un modèle de texte à ignorer. Les numéros de téléphone publics de votre organisation, les adresses e-mail du domaine de votre organisation et les exemples de données structurés que votre organisation utilise pour les tests en sont des exemples. Si vous utilisez ce type de liste, Macie ignore le texte qui correspond entièrement au modèle regex défini par la liste.

Pour ce type de liste, vous créez une expression régulière qui définit un modèle commun pour le texte qui n'est pas sensible mais qui varie ou est susceptible de changer. Contrairement à une liste de texte prédéfini, vous créez et stockez l'expression régulière et tous les autres paramètres de liste dans Macie. Vous pouvez ensuite créer et configurer des tâches de découverte de données sensibles pour utiliser la liste, ou ajouter la liste aux paramètres de découverte automatique de données sensibles de votre compte. Lorsque ces tâches sont exécutées ou

que Macie effectue une découverte automatique pour votre compte, Macie utilise la dernière version de l'expression régulière de la liste pour analyser les données. Si Macie trouve du texte qui correspond parfaitement au modèle défini par la liste, Macie ne signale pas cette occurrence de texte comme une donnée sensible.

Pour obtenir des exigences détaillées, des recommandations et des exemples de chaque type de liste, voirAutoriser les options et les exigences de la liste. Vous pouvez créer jusqu'à 10 listes d'autorisation pour votre compte dans chaque liste prise en charge Région AWS, jusqu'à cinq listes d'autorisation qui spécifient un texte prédéfini et jusqu'à cinq listes d'autorisation qui spécifient des expressions régulières. Vous pouvez créer et utiliser des listes d'autorisation dans tous les Régions AWS endroits où Macie est actuellement disponible, à l'exception de la région Asie-Pacifique (Osaka).

Pour créer et gérer des listes d'autorisations, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie. Les rubriques suivantes expliquent comment procéder. Pour l'API, les rubriques incluent des exemples expliquant comment effectuer ces tâches à l'aide de AWS Command Line Interface (AWS CLI). Vous pouvez également effectuer ces tâches en utilisant la version actuelle d'un autre outil de ligne de AWS commande ou d'un AWS SDK, ou en envoyant des requêtes HTTPS directement à Macie. Pour plus d'informations sur AWS les outils et les SDK, consultez la section Outils sur AWS lesquels vous pouvez vous appuyer.

Rubriques

- Création de listes d'autorisation
- Vérification de l'état des listes d'autorisation
- Modification des listes d'autorisations
- Supprimer des listes d'autorisation

Création de listes d'autorisation

La manière dont vous créez une liste d'autorisation dans Amazon Macie dépend du type de liste que vous souhaitez créer. Une liste d'autorisation peut être un fichier qui répertorie le texte prédéfini à ignorer ou une expression régulière (regex) qui définit un modèle de texte à ignorer. Choisissez la section correspondant au type de liste que vous souhaitez créer.

Texte prédéfini

Avant de créer ce type de liste d'autorisation dans Macie, procédez comme suit :

1. À l'aide d'un éditeur de texte, créez un fichier texte brut délimité par des lignes répertoriant le texte spécifique à ignorer, par exemple un fichier .txt, .text ou .plain. Pour plus d'informations, consultez Exigences de syntaxe pour les listes de texte prédéfini.
2. Téléchargez le fichier dans un compartiment S3 à usage général et notez le nom du compartiment et de l'objet. Vous devez saisir ces noms lorsque vous configurez les paramètres dans Macie.
3. Assurez-vous que les paramètres du compartiment et de l'objet S3 vous permettent, à vous et à Macie, de récupérer la liste depuis le compartiment. Pour plus d'informations, consultez Exigences de stockage pour les listes de texte prédéfini.
4. Si vous avez chiffré l'objet S3, assurez-vous qu'il est chiffré avec une clé que vous et Macie êtes autorisés à utiliser. Pour plus d'informations, consultez Exigences de chiffrement/déchiffrement pour les listes de texte prédéfini.

Après avoir effectué ces étapes, vous êtes prêt à configurer les paramètres de la liste dans Macie. Vous pouvez configurer les paramètres à l'aide de la console Amazon Macie ou de l'API Amazon Macie.

Console

Suivez ces étapes pour configurer les paramètres d'une liste d'autorisations à l'aide de la console Amazon Macie.

Pour configurer les paramètres de liste d'autorisation dans Macie

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, sous Paramètres, sélectionnez Autoriser les listes.
3. Sur la page Autoriser les listes, choisissez Créer.
4. Sous Sélectionnez un type de liste, choisissez Texte prédéfini.
5. Sous Paramètres de liste, utilisez les options suivantes pour saisir des paramètres supplémentaires pour la liste d'autorisation :
   - Dans Nom, entrez le nom de la liste. Le nom peut contenir jusqu'à 128 caractères.
   - Dans Description, entrez éventuellement une brève description de la liste. La description peut contenir jusqu'à 512 caractères.
   - Pour le nom du compartiment S3, entrez le nom du compartiment qui stocke la liste.

Dans Amazon S3, vous pouvez trouver cette valeur dans le champ Nom des propriétés du compartiment. Cette valeur est sensible à la casse. En outre, n'utilisez pas de caractères génériques ou de valeurs partielles lorsque vous entrez le nom.

- Pour le nom de l'objet S3, entrez le nom de l'objet S3 qui stocke la liste.

  Dans Amazon S3, vous pouvez trouver cette valeur dans le champ Clé des propriétés de l'objet. Si le nom inclut un chemin, veillez à inclure le chemin complet lorsque vous entrez le nom, par exemple**`allowlists/macie/mylist.txt`**. Cette valeur est sensible à la casse. En outre, n'utilisez pas de caractères génériques ou de valeurs partielles lorsque vous entrez le nom.

6. (Facultatif) Sous Balises, choisissez Ajouter une étiquette, puis entrez jusqu'à 50 balises à attribuer à la liste d'autorisation.

   Un tag est un label que vous définissez et attribuez à certains types de AWS ressources. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Les balises peuvent vous aider à identifier, à classer et à gérer les ressources de différentes manières, par exemple en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Pour en savoir plus, veuillez consulter la section Marquage des ressources Amazon Macie.

7. Lorsque vous avez terminé, choisissez Create (Créer).

Macie teste les paramètres de la liste. Macie vérifie également qu'il peut récupérer la liste depuis Amazon S3 et analyser le contenu de la liste. Si une erreur se produit, Macie affiche un message décrivant l'erreur. Pour obtenir des informations détaillées qui peuvent vous aider à résoudre l'erreur, consultezOptions et exigences relatives aux listes de texte prédéfini. Une fois les erreurs corrigées, vous pouvez enregistrer les paramètres de la liste.

API

Pour configurer les paramètres des listes d'autorisation par programmation, utilisez CreateAllowListl'API Amazon Macie et spécifiez les valeurs appropriées pour les paramètres requis.

Pour le `criteria` paramètre, utilisez un `s3WordsList` objet pour spécifier le nom du compartiment S3 (`bucketName`) et le nom de l'objet S3 (`objectKey`) qui stocke la liste. Pour déterminer le nom du compartiment, reportez-vous au `Name` champ dans Amazon S3. Pour déterminer le nom de l'objet, reportez-vous au `Key` champ dans Amazon S3. Notez que

ces valeurs distinguent les majuscules et minuscules. En outre, n'utilisez pas de caractères génériques ou de valeurs partielles lorsque vous spécifiez ces noms.

Pour configurer les paramètres à l'aide de AWS CLI, exécutez la create-allow-listcommande et spécifiez les valeurs appropriées pour les paramètres requis. Les exemples suivants montrent comment configurer les paramètres d'une liste d'autorisations stockée dans un compartiment S3 nommé *DOC-EXAMPLE-BUCKET*. Le nom de l'objet S3 qui stocke la liste est *allowlists/macie/mylist.txt*.

Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws macie2 create-allow-list \
--criteria '{"s3WordsList":{"bucketName":"DOC-EXAMPLE-
BUCKET","objectKey":"allowlists/macie/mylist.txt"}}' \
--name my_allow_list \
--description "Lists public phone numbers and names for Example Corp."
```

Cet exemple est formaté pour Microsoft Windows et utilise le caractère de continuation de ligne caret (^) pour améliorer la lisibilité.

```
C:\> aws macie2 create-allow-list ^
--criteria={\"s3WordsList\":{\"bucketName\":\"DOC-EXAMPLE-BUCKET\",\"objectKey\":
\"allowlists/macie/mylist.txt\"}} ^
--name my_allow_list ^
--description "Lists public phone numbers and names for Example Corp."
```

Lorsque vous soumettez votre demande, Macie teste les paramètres de la liste. Macie vérifie également qu'il peut récupérer la liste depuis Amazon S3 et analyser le contenu de la liste. Si une erreur se produit, votre demande échoue et Macie renvoie un message décrivant l'erreur. Pour obtenir des informations détaillées qui peuvent vous aider à résoudre l'erreur, consultezOptions et exigences relatives aux listes de texte prédéfini.

Si Macie peut récupérer et analyser la liste, votre demande aboutit et vous recevez un résultat similaire à ce qui suit.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
nkr81bmtu2542yyexample",
    "id": "nkr81bmtu2542yyexample"
```

```
}
```

Où se `arn` trouve le nom de ressource Amazon (ARN) de la liste d'autorisation créée et `id` l'identifiant unique de la liste.

Après avoir enregistré les paramètres de la liste, vous pouvez créer et configurer des tâches de découverte de données sensibles pour utiliser la liste, ou ajouter la liste à vos paramètres de découverte automatique de données sensibles. Chaque fois que ces tâches commencent à s'exécuter ou qu'un cycle d'analyse de découverte automatique démarre, Macie récupère la dernière version de la liste sur Amazon S3. Macie utilise ensuite cette version de la liste lorsqu'il analyse les données.

Expression régulière

Lorsque vous créez une liste d'autorisation qui spécifie une expression régulière (regex), vous définissez l'expression régulière et tous les autres paramètres de liste directement dans Macie. Macie prend en charge un sous-ensemble de la syntaxe du modèle regex fournie par la bibliothèque Perl Compatible Regular Expressions (PCRE). Pour plus d'informations, consultez Support syntaxique et recommandations.

Vous pouvez créer ce type de liste à l'aide de la console Amazon Macie ou de l'API Amazon Macie.

Console

Suivez ces étapes pour créer une liste d'autorisations à l'aide de la console Amazon Macie.

Pour créer une liste d'autorisations

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, sous Paramètres, sélectionnez Autoriser les listes.
3. Sur la page Autoriser les listes, choisissez Créer.
4. Sous Sélectionnez un type de liste, choisissez Expression régulière.
5. Sous Paramètres de liste, utilisez les options suivantes pour saisir des paramètres supplémentaires pour la liste d'autorisation :
   - Dans Nom, entrez le nom de la liste. Le nom peut contenir jusqu'à 128 caractères.
   - Dans Description, entrez éventuellement une brève description de la liste. La description peut contenir jusqu'à 512 caractères.

- Pour Expression régulière, entrez l'expression régulière qui définit le modèle de texte à ignorer. L'expression régulière peut contenir jusqu'à 512 caractères.

6. (Facultatif) Pour Evaluate, entrez jusqu'à 1 000 caractères dans la zone Exemple de données, puis choisissez Test pour tester l'expression régulière. Macie évalue les exemples de données et indique le nombre d'occurrences de texte correspondant à l'expression régulière. Vous pouvez répéter cette étape autant de fois que vous le souhaitez pour affiner et optimiser l'expression régulière.

   > **Note**
   >
   > Nous vous recommandons de tester et d'affiner l'expression régulière avec plusieurs ensembles d'échantillons de données. Si vous créez une expression régulière trop générale, Macie risque d'ignorer les occurrences de texte que vous considérez comme sensibles. Si une expression régulière est trop spécifique, Macie peut ne pas ignorer les occurrences de texte que vous ne considérez pas comme sensibles.

7. (Facultatif) Sous Balises, choisissez Ajouter une étiquette, puis entrez jusqu'à 50 balises à attribuer à la liste d'autorisation.

   Un tag est un label que vous définissez et attribuez à certains types de AWS ressources. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Les balises peuvent vous aider à identifier, à classer et à gérer les ressources de différentes manières, par exemple en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Pour en savoir plus, veuillez consulter la section Marquage des ressources Amazon Macie.

8. Lorsque vous avez terminé, choisissez Create (Créer).

Macie teste les paramètres de la liste. Macie teste également l'expression régulière pour vérifier qu'elle peut compiler l'expression. Si une erreur se produit, Macie affiche un message décrivant l'erreur. Pour obtenir des informations détaillées qui peuvent vous aider à résoudre l'erreur, consultezOptions et exigences relatives aux expressions régulières dans les listes d'autorisation. Une fois les erreurs corrigées, vous pouvez enregistrer la liste des autorisations.

API

Avant de créer ce type de liste d'autorisation dans Macie, nous vous recommandons de tester et d'affiner l'expression régulière à l'aide de plusieurs ensembles d'échantillons de données. Si vous créez une expression régulière trop générale, Macie risque d'ignorer les occurrences de texte que

vous considérez comme sensibles. Si une expression régulière est trop spécifique, Macie peut ne pas ignorer les occurrences de texte que vous ne considérez pas comme sensibles.

Pour tester une expression avec Macie, vous pouvez utiliser le TestCustomDataIdentifierfonctionnement de l'API Amazon Macie ou, dans le cas contraire, exécuter AWS CLItest-custom-data-identifierla commande. Macie utilise le même code sous-jacent pour compiler des expressions pour les listes d'autorisation et les identificateurs de données personnalisés. Si vous testez une expression de cette manière, veillez à ne spécifier des valeurs que pour les `sampleText` paramètres `regex` et. Dans le cas contraire, vous recevrez des résultats inexacts.

Lorsque vous êtes prêt à créer ce type de liste d'autorisations, utilisez CreateAllowListl'API Amazon Macie et spécifiez les valeurs appropriées pour les paramètres requis. Pour le `criteria` paramètre, utilisez le `regex` champ pour spécifier l'expression régulière qui définit le modèle de texte à ignorer. L'expression peut contenir jusqu'à 512 caractères.

Pour créer ce type de liste à l'aide de AWS CLI, exécutez la create-allow-listcommande et spécifiez les valeurs appropriées pour les paramètres requis. Les exemples suivants créent une liste d'autorisations nommée *`my_allow_list`*. L'expression régulière est conçue pour ignorer toutes les adresses e-mail qu'un identifiant de données personnalisé pourrait autrement détecter pour le `example.com` domaine.

Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne barre oblique inverse (\) pour améliorer la lisibilité.

```
$ aws macie2 create-allow-list \
--criteria '{"regex":"[a-z]@example.com"}' \
--name my_allow_list \
--description "Ignores all email addresses for Example Corp."
```

Cet exemple est formaté pour Microsoft Windows et utilise le caractère de continuation de ligne caret (^) pour améliorer la lisibilité.

```
C:\> aws macie2 create-allow-list ^
--criteria={\"regex\":\"[a-z]@example.com\"} ^
--name my_allow_list ^
--description "Ignores all email addresses for Example Corp."
```

Lorsque vous soumettez votre demande, Macie teste les paramètres de la liste. Macie teste également l'expression régulière pour vérifier qu'elle peut compiler l'expression. Si une erreur se

produit, la demande échoue et Macie renvoie un message décrivant l'erreur. Pour obtenir des informations détaillées qui peuvent vous aider à résoudre l'erreur, consultezOptions et exigences relatives aux expressions régulières dans les listes d'autorisation.

Si Macie parvient à compiler l'expression, la demande aboutit et vous recevez un résultat similaire à ce qui suit :

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
    "id": "km2d4y22hp6rv05example"
}
```

Où se `arn` trouve le nom de ressource Amazon (ARN) de la liste d'autorisation créée et `id` l'identifiant unique de la liste.

Après avoir enregistré la liste, vous pouvez créer et configurer des tâches de découverte de données sensibles pour l'utiliser, ou l'ajouter à vos paramètres de découverte automatique de données sensibles. Lorsque ces tâches sont exécutées ou que Macie effectue une découverte automatique pour votre compte, Macie utilise la dernière version de l'expression régulière de la liste pour analyser les données.

Vérification de l'état des listes d'autorisation

Il est important de vérifier régulièrement l'état de vos listes d'autorisations. Dans le cas contraire, des erreurs peuvent amener Amazon Macie à produire des résultats d'analyse inattendus, tels que des résultats de données sensibles pour le texte que vous avez spécifié dans une liste d'autorisation.

Si vous configurez une tâche de découverte de données sensibles pour utiliser une liste d'autorisation et que Macie ne peut pas accéder à la liste ou l'utiliser lorsque la tâche commence à s'exécuter, la tâche continue de s'exécuter. Cependant, Macie n'utilise pas la liste lorsqu'il analyse des objets S3. De même, si un cycle d'analyse démarre pour la découverte automatique de données sensibles et que Macie ne peut pas accéder à une liste d'autorisation spécifiée ou l'utiliser, l'analyse se poursuit mais Macie n'utilise pas la liste.

Il est peu probable que des erreurs se produisent pour une liste d'autorisation qui spécifie une expression régulière (regex). Cela s'explique en partie par le fait que Macie teste automatiquement l'expression régulière lorsque vous créez ou mettez à jour les paramètres de la liste. De plus, vous stockez l'expression régulière et tous les autres paramètres de liste dans Macie.

Cependant, des erreurs peuvent se produire pour une liste d'autorisation qui spécifie un texte prédéfini, en partie parce que vous stockez la liste dans Amazon S3 plutôt que dans Macie. Les causes d'erreurs les plus courantes sont les suivantes :

- Le compartiment ou l'objet S3 est supprimé.
- Le compartiment ou l'objet S3 est renommé et les paramètres de la liste dans Macie ne spécifient pas le nouveau nom.
- Les paramètres d'autorisation du compartiment S3 sont modifiés et Macie perd l'accès au compartiment et à l'objet.
- Les paramètres de chiffrement du compartiment S3 sont modifiés et Macie ne peut pas déchiffrer l'objet qui stocke la liste.
- La politique relative à la clé de chiffrement est modifiée et Macie perd l'accès à la clé. Macie ne peut pas déchiffrer l'objet S3 qui stocke la liste.

> **Important**
>
> Étant donné que ces erreurs affectent les résultats de vos analyses, nous vous recommandons de vérifier régulièrement l'état de vos listes d'autorisation. Nous vous recommandons de le faire également si vous modifiez les autorisations ou les paramètres de chiffrement d'un compartiment S3 qui stocke une liste d'autorisations, ou si vous modifiez la politique d'une clé AWS Key Management Service (AWS KMS) utilisée pour chiffrer une liste.

Vous pouvez vérifier l'état de vos listes d'autorisations à l'aide de la console Amazon Macie ou de l'API Amazon Macie. Pour obtenir des informations détaillées qui peuvent vous aider à résoudre les erreurs qui se produisent, consultezOptions et exigences relatives aux listes de texte prédéfini.

Console

Suivez ces étapes pour vérifier l'état de vos listes d'autorisation à l'aide de la console Amazon Macie.

Pour vérifier l'état de vos listes d'autorisations

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, sous Paramètres, sélectionnez Autoriser les listes.

3. Sur la page Autoriser les listes, choisissez Actualiser
().
Macie teste les paramètres de toutes vos listes d'autorisation et met à jour le champ État pour indiquer le statut actuel de chaque liste.

   Si une liste spécifie une expression régulière, son statut est généralement OK. Cela signifie que Macie peut compiler l'expression. Si une liste contient un texte prédéfini, son statut peut être l'une des valeurs suivantes.

   OK

   Macie peut récupérer et analyser le contenu de la liste.

   Accès refusé

   Macie n'est pas autorisé à accéder à l'objet S3 qui stocke la liste. Amazon S3 a refusé la demande de récupération de l'objet. Une liste peut également avoir ce statut si l'objet est chiffré par un client géré AWS KMS key que Macie n'est pas autorisé à utiliser.

   Pour corriger cette erreur, consultez la politique du compartiment et les autres paramètres d'autorisation pour le compartiment et l'objet. Assurez-vous que Macie est autorisé à accéder à l'objet et à le récupérer. Si l'objet est chiffré à l'aide d'une AWS KMS clé gérée par le client, consultez également la politique relative aux clés et assurez-vous que Macie est autorisé à utiliser la clé.

   Error (Erreur)

   Une erreur temporaire ou interne s'est produite lorsque Macie a tenté de récupérer ou d'analyser le contenu de la liste. Une liste d'autorisation peut également avoir ce statut si elle est chiffrée à l'aide d'une clé de chiffrement à laquelle Amazon S3 et Macie ne peuvent pas accéder ou utiliser.

   Pour corriger cette erreur, attendez quelques minutes, puis choisissez à nouveau refresh
   ().
   Si le statut reste Erreur, vérifiez les paramètres de chiffrement de l'objet S3. Assurez-vous que l'objet est chiffré avec une clé à laquelle Amazon S3 et Macie peuvent accéder et utiliser.

L'objet est vide

Macie peut récupérer la liste depuis Amazon S3, mais elle ne contient aucun contenu.

Pour corriger cette erreur, téléchargez l'objet depuis Amazon S3 et assurez-vous qu'il contient les entrées correctes. Si les entrées sont correctes, vérifiez les paramètres de la liste dans Macie. Assurez-vous que les noms de bucket et d'objet spécifiés sont corrects.

Objet introuvable

La liste n'existe pas dans Amazon S3.

Pour corriger cette erreur, passez en revue les paramètres de la liste dans Macie. Assurez-vous que les noms de bucket et d'objet spécifiés sont corrects.

Quota dépassé

Macie peut accéder à la liste dans Amazon S3. Toutefois, le nombre d'entrées de la liste ou la taille de stockage de la liste dépasse le quota d'une liste autorisée.

Pour corriger cette erreur, divisez la liste en plusieurs fichiers. Assurez-vous que chaque fichier contient moins de 100 000 entrées. Assurez-vous également que la taille de chaque fichier est inférieure à 35 Mo. Chargez ensuite chaque fichier sur Amazon S3. Lorsque vous avez terminé, configurez les paramètres de liste d'autorisation dans Macie pour chaque fichier. Vous pouvez avoir jusqu'à cinq listes de texte prédéfini dans chacune des listes prises en charge Région AWS.

Étranglé

Amazon S3 a limité la demande de récupération de la liste.

Pour corriger cette erreur, attendez quelques minutes, puis choisissez à nouveau refresh ().

Accès utilisateur refusé

Amazon S3 a refusé la demande de récupération de l'objet. Si l'objet spécifié existe, vous n'êtes pas autorisé à y accéder ou s'il est chiffré avec une AWS KMS clé que vous n'êtes pas autorisé à utiliser.

Pour corriger cette erreur, AWS contactez votre administrateur pour vous assurer que les paramètres de la liste spécifient les noms de bucket et d'objet corrects et que vous

disposez d'un accès en lecture au bucket et à l'objet. Si l'objet est chiffré, assurez-vous qu'il l'est avec une clé que vous avez l'autorisation d'utiliser.

4. Pour consulter les paramètres et le statut d'une liste spécifique, choisissez le nom de la liste.

API

Pour vérifier l'état d'une liste d'autorisations par programmation, utilisez l'GetAllowListAPI Amazon Macie ou, pour AWS CLI le, exécutez la commande. get-allow-list

Pour le `id` paramètre, spécifiez l'identifiant unique de la liste d'autorisation dont vous souhaitez vérifier le statut. Pour obtenir cet identifiant, vous pouvez utiliser l'ListAllowListsopération. L'ListAllowListsopération permet de récupérer des informations sur toutes les listes d'autorisations associées à votre compte. Si vous utilisez le AWS CLI, vous pouvez exécuter la list-allow-listscommande pour récupérer ces informations.

Lorsque vous soumettez une GetAllowList demande, Macie teste tous les paramètres de la liste d'autorisation. Si les paramètres spécifient une expression régulière (regex), Macie vérifie qu'il peut compiler l'expression. Si les paramètres spécifient une liste de texte prédéfini, Macie vérifie qu'il peut récupérer et analyser la liste.

Macie renvoie ensuite un `GetAllowListResponse` objet qui fournit les détails de la liste des autorisations. Dans l'`GetAllowListResponse`objet, l'`status`objet indique l'état actuel de la liste : un code d'état (`code`) et, selon le code d'état, une brève description de l'état de la liste (`description`).

Si la liste d'autorisation spécifie une expression régulière, le code d'état est généralement le cas `OK` et aucune description n'est associée. Cela signifie que Macie a correctement compilé l'expression.

Si la liste d'autorisation indique un texte prédéfini, le code d'état varie en fonction des résultats du test :

- Si Macie a récupéré et analysé la liste avec succès, le code d'état est valide `OK` et il n'y a pas de description associée.
- Si une erreur a empêché Macie de récupérer ou d'analyser la liste, le code d'état et la description indiquent la nature de l'erreur survenue.

Pour obtenir la liste des codes de statut possibles et une description de chacun d'entre eux, consultez AllowListStatusle manuel Amazon Macie API Reference.

Modification des listes d'autorisations

Après avoir créé une liste d'autorisations, vous pouvez modifier la plupart des paramètres de la liste dans Amazon Macie. Par exemple, vous pouvez modifier le nom et la description de la liste, et vous pouvez ajouter et modifier les balises de la liste. Le seul paramètre que vous ne pouvez pas modifier est le type de liste. Par exemple, si une liste d'autorisation existante spécifie une expression régulière, vous ne pouvez pas remplacer son type par du texte prédéfini.

Si une liste d'autorisation indique un texte prédéfini, vous pouvez également modifier les entrées de la liste. Pour ce faire, mettez à jour le fichier qui contient les entrées, puis chargez la nouvelle version du fichier sur Amazon S3. La prochaine fois que Macie se prépare à utiliser la liste, Macie récupère la dernière version du fichier sur Amazon S3. Lorsque vous chargez le nouveau fichier, assurez-vous de le stocker dans le même compartiment et le même objet S3. Ou, si vous modifiez le nom du bucket ou de l'objet, assurez-vous de mettre à jour les paramètres de la liste dans Macie.

Vous pouvez modifier les paramètres d'une liste d'autorisations à l'aide de la console Amazon Macie ou de l'API Amazon Macie.

Console

Procédez comme suit pour modifier les paramètres d'une liste d'autorisations à l'aide de la console Amazon Macie.

Pour modifier une liste d'autorisations

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, sous Paramètres, sélectionnez Autoriser les listes.
3. Sur la page Listes autorisées, choisissez le nom de la liste autorisée que vous souhaitez modifier. La page de liste d'autorisation s'ouvre et affiche les paramètres actuels de la liste.
4. Pour attribuer ou modifier des balises pour la liste d'autorisation, choisissez Gérer les balises dans la section Balises. Modifiez ensuite les balises si nécessaire. Lorsque vous avez terminé, choisissez Enregistrer.
5. Pour modifier les autres paramètres de la liste d'autorisation, choisissez Modifier dans la section Paramètres de la liste. Modifiez ensuite les paramètres souhaités :

- Nom — Entrez un nouveau nom pour la liste. Le nom peut contenir jusqu'à 128 caractères.
- Description — Entrez une nouvelle description de la liste. La description peut contenir jusqu'à 512 caractères.
- Si la liste des autorisations indique un texte prédéfini :
  - Nom du compartiment S3 : entrez le nom du compartiment qui stocke actuellement la liste.

    Dans Amazon S3, vous pouvez trouver cette valeur dans le champ Nom des propriétés du compartiment. Cette valeur est sensible à la casse. En outre, n'utilisez pas de caractères génériques ou de valeurs partielles lorsque vous entrez le nom.
  - Nom de l'objet S3 — Entrez le nom de l'objet S3 qui stocke actuellement la liste.

    Dans Amazon S3, vous pouvez trouver cette valeur dans le champ Clé des propriétés de l'objet. Si le nom inclut un chemin, veillez à inclure le chemin complet lorsque vous entrez le nom, par exemple**`allowlists/macie/mylist.txt`**. Cette valeur est sensible à la casse. En outre, n'utilisez pas de caractères génériques ou de valeurs partielles lorsque vous entrez le nom.
- Si la liste d'autorisation spécifie une expression régulière (regex), entrez une nouvelle expression régulière dans la zone Expression régulière. L'expression régulière peut contenir jusqu'à 512 caractères.

  Après avoir saisi la nouvelle expression régulière, testez-la éventuellement. Pour ce faire, entrez jusqu'à 1 000 caractères dans la zone Exemple de données, puis choisissez Test. Macie évalue les exemples de données et indique le nombre d'occurrences de texte correspondant à l'expression régulière. Vous pouvez répéter cette étape autant de fois que vous le souhaitez pour affiner et optimiser l'expression régulière avant d'enregistrer vos modifications.

Lorsque vous avez fini de modifier les paramètres, choisissez Enregistrer.

Macie teste les paramètres de la liste. Pour une liste de texte prédéfini, Macie vérifie également qu'il peut récupérer la liste depuis Amazon S3 et analyser le contenu de la liste. Pour une expression régulière, Macie vérifie également qu'il peut compiler l'expression. Si une erreur se produit, Macie affiche un message décrivant l'erreur. Pour obtenir des informations détaillées qui

peuvent vous aider à résoudre l'erreur, consultezAutoriser les options et les exigences de la liste. Une fois les erreurs corrigées, vous pouvez enregistrer vos modifications.

API

Pour modifier une liste d'autorisations par programmation, utilisez l'UpdateAllowListAPI Amazon Macie ou, pour AWS CLI le, exécutez la commande. update-allow-list Dans votre demande, utilisez les paramètres pris en charge pour spécifier une nouvelle valeur pour chaque paramètre que vous souhaitez modifier. Notez que les `name` paramètres `criteriaid`, et sont obligatoires. Si vous ne souhaitez pas modifier la valeur d'un paramètre obligatoire, spécifiez la valeur actuelle du paramètre.

Par exemple, la commande suivante modifie le nom et la description d'une liste d'autorisations existante. L'exemple est formaté pour Microsoft Windows et utilise le caractère de continuation de ligne caret (^) pour améliorer la lisibilité.

```
C:\> aws macie2 update-allow-list ^
--id km2d4y22hp6rv05example ^
--name my_allow_list-email ^
--criteria={\"regex\":\"[a-z]@example.com\"} ^
--description "Ignores all email addresses for the example.com domain"
```

Où :

- *km2d4y22hp6rv05example* est l'identifiant unique de la liste.
- *my_allow_list-email* est le nouveau nom de la liste.
- *[a-z] @example .com* est le critère de la liste, une expression régulière.
- *Ignore toutes les adresses e-mail pour le domaine exemple.com* est la nouvelle description de la liste.

Lorsque vous soumettez votre demande, Macie teste les paramètres de la liste. Si la liste contient du texte prédéfini, cela implique de vérifier que Macie peut récupérer la liste depuis Amazon S3 et analyser le contenu de la liste. Si la liste indique une expression régulière, cela implique de vérifier que Macie peut compiler l'expression.

Si une erreur se produit lorsque Macie teste les paramètres, votre demande échoue et Macie renvoie un message décrivant l'erreur. Pour obtenir des informations détaillées qui peuvent vous aider à résoudre l'erreur, consultezAutoriser les options et les exigences de la liste. Si la demande

échoue pour une autre raison, Macie renvoie une réponse HTTP 4 xx ou 500 indiquant pourquoi l'opération a échoué.

Si votre demande aboutit, Macie met à jour les paramètres de la liste et vous recevez un résultat similaire à ce qui suit.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:allow-list/
km2d4y22hp6rv05example",
    "id": "km2d4y22hp6rv05example"
}
```

Où se `arn` trouve le nom de ressource Amazon (ARN) de la liste d'autorisation mise à jour et `id` l'identifiant unique de la liste.

Supprimer des listes d'autorisation

Lorsque vous supprimez une liste d'autorisations dans Amazon Macie, vous supprimez définitivement tous les paramètres de la liste. Ces paramètres ne peuvent pas être restaurés après leur suppression. Si les paramètres spécifient une liste de textes prédéfinis que vous stockez dans Amazon S3, Macie ne supprime pas l'objet S3 qui stocke la liste. Seuls les paramètres de Macie sont supprimés.

Si vous configurez des tâches de découverte de données sensibles pour utiliser une liste d'autorisation et que vous supprimez ensuite la liste, les tâches s'exécuteront comme prévu. Toutefois, les résultats de votre tâche, qu'il s'agisse de la découverte de données sensibles ou de la découverte de données sensibles, peuvent indiquer un texte que vous avez précédemment spécifié dans une liste d'autorisation. De même, si vous configurez la découverte automatique des données sensibles pour utiliser une liste et que vous supprimez ensuite la liste, les cycles d'analyse quotidiens se poursuivront. Toutefois, les résultats relatifs à des données sensibles, les statistiques ou d'autres types de résultats peuvent indiquer un texte que vous avez précédemment spécifié dans une liste d'autorisation.

Avant de supprimer une liste d'autorisations, nous vous recommandons de consulter votre inventaire des tâches afin d'identifier les tâches qui utilisent cette liste et dont l'exécution est prévue dans le futur. Dans l'inventaire, le panneau de détails indique si une tâche est configurée pour utiliser des listes d'autorisation et, dans l'affirmative, lesquelles. Vérifiez également vos paramètres de découverte automatique des données sensibles. Il se peut que vous décidiez qu'il est préférable de modifier une liste plutôt que de la supprimer.

Comme mesure de protection supplémentaire, Macie vérifie les paramètres de toutes vos tâches lorsque vous essayez de supprimer une liste d'autorisations. Si vous avez configuré des tâches pour utiliser la liste et que l'une de ces tâches a un statut autre que Terminé ou Annulé, Macie ne supprime pas la liste à moins que vous ne fournissiez une confirmation supplémentaire.

Vous pouvez supprimer une liste d'autorisations à l'aide de la console Amazon Macie ou de l'API Amazon Macie.

Console

Procédez comme suit pour supprimer une liste d'autorisations à l'aide de la console Amazon Macie.

Pour supprimer une liste d'autorisations

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, sous Paramètres, sélectionnez Autoriser les listes.
3. Sur la page Listes autorisées, cochez la case correspondant à la liste autorisée que vous souhaitez supprimer.
4. Dans le menu Actions, sélectionnez Delete (Supprimer).
5. Lorsque vous êtes invité à confirmer, saisissez **`delete`**, puis choisissez Delete (Supprimer).

API

Pour supprimer une liste d'autorisations par programmation, utilisez l'DeleteAllowListAPI Amazon Macie. Pour le `id` paramètre, spécifiez l'identifiant unique de la liste d'autorisations à supprimer. Vous pouvez obtenir cet identifiant en utilisant l'ListAllowListsopération. L'ListAllowListsopération permet de récupérer des informations sur toutes les listes d'autorisations associées à votre compte. Si vous utilisez le AWS CLI, vous pouvez exécuter la list-allow-listscommande pour récupérer ces informations.

Pour le `ignoreJobChecks` paramètre, spécifiez si vous souhaitez forcer la suppression de la liste, même si les tâches de découverte de données sensibles sont configurées pour utiliser la liste :

- Si vous le spécifiez`false`, Macie vérifie les paramètres de toutes vos tâches dont le statut est autre que `COMPLETE` ou`CANCELLED`. Si aucune de ces tâches n'est configurée pour utiliser la liste, Macie la supprime définitivement. Si l'une de ces tâches est configurée pour utiliser la

liste, Macie rejette votre demande et renvoie une erreur HTTP 400 (`ValidationException`). Le message d'erreur indique le nombre de tâches applicables pour un maximum de 200 tâches.

- Si vous le spécifiez`true`, Macie supprime définitivement la liste sans vérifier les paramètres d'aucune de vos tâches.

Pour supprimer une liste d'autorisations à l'aide de AWS CLI, exécutez la delete-allow-listcommande. Par exemple :

```
C:\> aws macie2 delete-allow-list --id nkr81bmtu2542yyexample --ignore-job-checks
 false
```

Où *nkr81bmtu2542yyexample* est l'identifiant unique de la liste d'autorisations à supprimer.

Si votre demande aboutit, Macie renvoie une réponse HTTP 200 vide. Sinon, Macie renvoie une réponse HTTP 4 xx ou 500 indiquant pourquoi l'opération a échoué.

Si la liste d'autorisation spécifie un texte prédéfini, vous pouvez éventuellement supprimer l'objet S3 qui stocke la liste. Cependant, la conservation de cet objet peut vous permettre de disposer d'un historique immuable des découvertes relatives aux données sensibles et des résultats de découverte dans le cadre d'audits ou d'enquêtes sur la confidentialité et la protection des données.

Réalisation de la découverte automatisée de données sensibles avec Amazon Macie

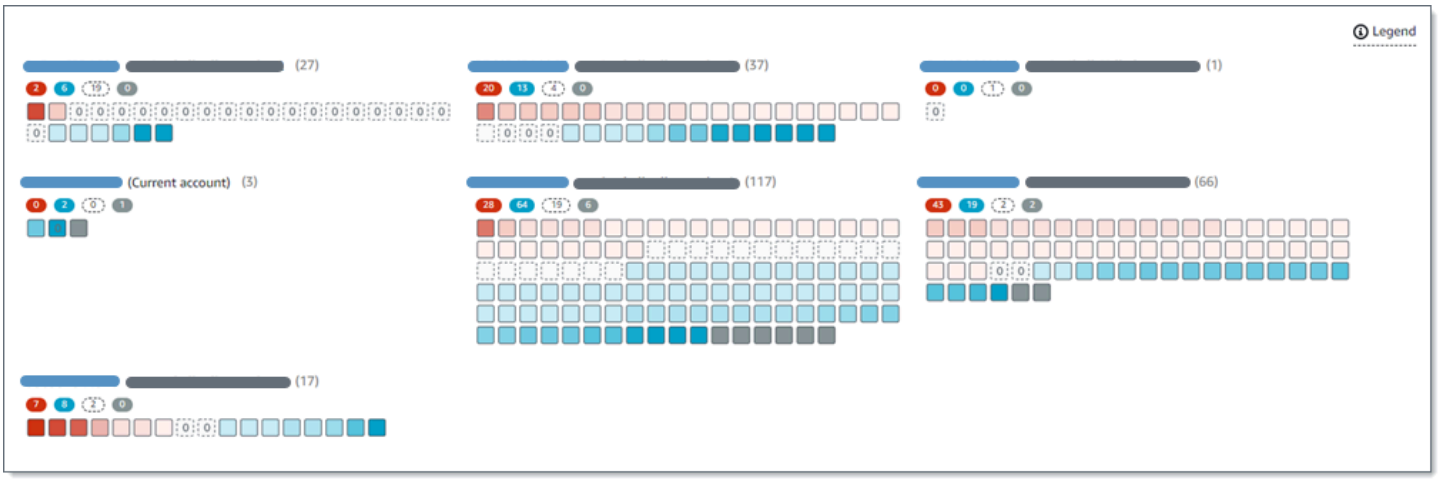
Pour avoir une visibilité étendue sur l'emplacement des données sensibles dans votre parc de données Amazon Simple Storage Service (Amazon S3), configurez Amazon Macie pour qu'il effectue une découverte automatique des données sensibles pour votre compte ou votre organisation. Grâce à la découverte automatique des données sensibles, Macie évalue en permanence votre inventaire de compartiments S3 et utilise des techniques d'échantillonnage pour identifier et sélectionner des objets S3 représentatifs dans vos compartiments. Macie récupère et analyse ensuite les objets sélectionnés, en les inspectant pour détecter la présence de données sensibles.

Par défaut, Macie sélectionne et analyse les objets de tous vos compartiments S3 à usage général. Si vous êtes l'administrateur Macie d'une organisation, cela inclut les objets contenus dans des compartiments détenus par vos comptes membres. Vous pouvez ajuster la portée des analyses en excluant des compartiments spécifiques, par exemple les compartiments qui stockent généralement

les données de journalisation. AWS Si vous êtes un administrateur Macie, une option supplémentaire consiste à activer ou à désactiver la découverte automatique des données sensibles pour case-by-case les comptes individuels de votre organisation.

Vous pouvez adapter les analyses pour qu'elles se concentrent sur des types spécifiques de données sensibles. Par défaut, Macie analyse les objets S3 à l'aide de l'ensemble d'identifiants de données gérés que nous recommandons pour la découverte automatique des données sensibles. Pour personnaliser les analyses, configurez Macie pour qu'il utilise des identifiants de données gérés spécifiques fournis par Macie, des identifiants de données personnalisés que vous définissez ou une combinaison des deux. Vous pouvez également affiner les analyses en configurant Macie pour qu'il utilise les listes d'autorisation que vous spécifiez.

Au fur et à mesure que l'analyse progresse chaque jour, Macie enregistre les données sensibles qu'elle trouve et les analyses qu'elle effectue : les résultats de données sensibles, qui signalent les données sensibles que Macie trouve dans des objets S3 individuels, et les résultats de découverte de données sensibles, qui enregistrent les détails de l'analyse des objets S3 individuels. Macie met également à jour les statistiques, les données d'inventaire et les autres informations qu'il fournit sur vos données Amazon S3. Par exemple, une carte thermique interactive sur la console fournit une représentation visuelle de la sensibilité des données dans l'ensemble de votre parc de données :



Ces fonctionnalités sont conçues pour vous aider à évaluer la sensibilité des données dans l'ensemble de votre parc de données Amazon S3, et à effectuer une analyse approfondie pour étudier et évaluer des comptes, des compartiments et des objets individuels. Ils peuvent également vous aider à déterminer où effectuer une analyse plus approfondie et plus immédiate en exécutant des tâches de découverte de données sensibles. Associées aux informations fournies par Macie concernant la sécurité et la confidentialité de vos données Amazon S3, vous pouvez également utiliser ces fonctionnalités pour identifier les cas où une correction immédiate pourrait être

nécessaire, par exemple un compartiment accessible au public dans lequel Macie a trouvé des données sensibles.

Pour configurer et gérer la découverte automatique des données sensibles, votre compte doit être le compte administrateur Macie d'une organisation ou un compte Macie autonome.

Rubriques

Comment fonctionne la découverte automatique des données sensibles

Lorsque vous activez Amazon Macie pour votre compte Compte AWS, Macie crée actuellement un rôle lié au service AWS Identity and Access Management (IAM) pour votre compte. Région AWS La politique d'autorisation pour ce rôle permet à Macie d'appeler d'autres personnes Services AWS et de surveiller AWS les ressources en votre nom. En utilisant ce rôle, Macie génère et gère un inventaire complet de vos compartiments à usage général Amazon Simple Storage Service (Amazon S3) dans la région. L'inventaire inclut des informations sur chacun de vos compartiments S3 et sur les objets qu'ils contiennent. Si vous êtes l'administrateur Macie d'une organisation, votre inventaire inclut des informations sur les compartiments que possèdent vos comptes membres. Pour plus d'informations, consultez Gestion de plusieurs comptes .

Si vous activez la découverte automatique des données sensibles, Macie évalue quotidiennement vos données d'inventaire afin d'identifier les objets S3 éligibles à la découverte automatique. Dans le cadre de l'évaluation, Macie sélectionne également un échantillon d'objets représentatifs à analyser. Macie récupère et analyse ensuite la dernière version de chaque objet sélectionné, en l'inspectant pour détecter les données sensibles.

Au fur et à mesure que l'analyse progresse chaque jour, Macie met à jour les statistiques, les données d'inventaire et les autres informations qu'il fournit sur vos données Amazon S3. Macie produit également des enregistrements des données sensibles qu'il trouve et des analyses qu'il

effectue. Les données obtenues permettent de savoir où Macie a trouvé des données sensibles dans votre patrimoine de données Amazon S3, qui peut couvrir tous les compartiments S3 à usage général que Macie surveille et analyse pour votre compte. Les données peuvent vous aider à évaluer la sécurité et la confidentialité de vos données Amazon S3, à déterminer où effectuer une enquête plus approfondie et à identifier les cas où des mesures correctives sont nécessaires.

Pour une brève démonstration du fonctionnement de la découverte automatique des données sensibles, regardez la vidéo suivante : Présentation de la découverte automatique des données par Amazon Macie.

Pour configurer et gérer la découverte automatique des données sensibles, votre compte doit être le compte administrateur Macie d'une organisation ou un compte Macie autonome. Si votre compte fait partie d'une organisation, seul l'administrateur Macie de votre organisation peut activer ou désactiver la découverte automatique des données sensibles pour les comptes de votre organisation. En outre, seul l'administrateur Macie peut configurer et gérer les paramètres de découverte automatique des données sensibles pour les comptes.

Rubriques

Composants clés

Amazon Macie utilise une combinaison de fonctionnalités et de techniques pour effectuer la découverte automatisée de données sensibles. Elles fonctionnent conjointement avec les fonctionnalités fournies par Macie pour vous aider à surveiller vos données Amazon S3 à des fins de sécurité et de contrôle d'accès.

Sélection des objets S3 à analyser

Macie évalue quotidiennement vos données d'inventaire Amazon S3 afin d'identifier les objets S3 susceptibles d'être analysés par découverte automatique de données sensibles. Si vous êtes l'administrateur Macie d'une organisation, l'évaluation inclut par défaut les données relatives aux compartiments S3 que possèdent vos comptes membres.

Dans le cadre de l'évaluation, Macie utilise des techniques d'échantillonnage pour sélectionner des objets S3 représentatifs à analyser. Les techniques définissent des groupes d'objets dotés de

métadonnées similaires et susceptibles d'avoir un contenu similaire. Les groupes sont basés sur des dimensions telles que le nom du compartiment, le préfixe, la classe de stockage, l'extension du nom de fichier et la date de dernière modification. Macie sélectionne ensuite un ensemble représentatif d'échantillons de chaque groupe, récupère la dernière version de chaque objet sélectionné sur Amazon S3 et analyse chaque objet sélectionné pour déterminer s'il contient des données sensibles. Lorsque l'analyse est terminée, Macie supprime sa copie de l'objet.

La stratégie d'échantillonnage donne la priorité aux analyses distribuées. En général, il utilise une approche axée sur l'étendue de votre parc de données Amazon S3. Chaque jour, un ensemble représentatif d'objets S3 est sélectionné parmi le plus grand nombre possible de compartiments à usage général en fonction de la taille de stockage totale de tous les objets classifiables de votre parc de données Amazon S3. Par exemple, si Macie a déjà analysé et trouvé des données sensibles dans des objets d'un compartiment et n'a pas encore analysé d'objets dans un autre compartiment, ce dernier compartiment est une priorité d'analyse plus élevée. Cette approche vous permet de mieux comprendre plus rapidement la sensibilité de vos données Amazon S3. En fonction de la taille de votre parc de données, les résultats d'analyse peuvent commencer à apparaître dans les 48 heures.

La stratégie d'échantillonnage donne également la priorité à l'analyse des différents types d'objets S3 et d'objets récemment créés ou modifiés. Il n'est pas garanti qu'un échantillon d'objet soit concluant. Par conséquent, l'analyse d'un ensemble diversifié d'objets peut permettre de mieux comprendre les types et la quantité de données sensibles qu'un compartiment S3 peut contenir. En outre, la hiérarchisation des objets nouveaux ou récemment modifiés permet à l'analyse de s'adapter aux modifications apportées à votre inventaire de compartiments. Par exemple, si des objets sont créés ou modifiés après une analyse précédente, ils sont prioritaires pour les analyses ultérieures. Inversement, si un objet a déjà été analysé et n'a pas changé depuis cette analyse, Macie ne l'analyse pas à nouveau. Cette approche vous permet d'établir des lignes de base de sensibilité pour des compartiments S3 individuels. Ensuite, au fur et à mesure que les analyses continues et progressives de votre compte progressent, vos évaluations de sensibilité des compartiments individuels peuvent devenir de plus en plus approfondies et détaillées à un rythme prévisible.

Définition de la portée des analyses

Par défaut, Macie inclut tous les compartiments S3 à usage général qu'il surveille et analyse pour votre compte lorsqu'il évalue vos données d'inventaire et sélectionne les objets S3 à analyser. Si vous êtes l'administrateur Macie d'une organisation, cela inclut les compartiments que possèdent vos comptes membres.

Vous pouvez ajuster la portée des analyses en excluant des compartiments S3 spécifiques. Par exemple, vous pouvez préférer exclure les compartiments qui stockent généralement des données de AWS journalisation, telles que les journaux AWS CloudTrail d'événements. Pour exclure un bucket, vous pouvez modifier les paramètres de découverte automatique des données sensibles pour votre compte ou le bucket. Dans ce cas, Macie commence à exclure le bucket au début du prochain cycle quotidien d'évaluation et d'analyse. Vous pouvez exclure jusqu'à 1 000 compartiments des analyses. Si vous excluez un compartiment S3, vous pouvez ensuite l'inclure à nouveau. Pour ce faire, modifiez à nouveau les paramètres de votre compte ou du bucket. Macie commence ensuite à inclure le godet au début du prochain cycle quotidien d'évaluation et d'analyse.

Si vous êtes l'administrateur Macie d'une organisation, vous pouvez également activer ou désactiver la découverte automatique des données sensibles pour les comptes individuels de votre organisation. Si vous désactivez la découverte automatique pour un compte, Macie exclut tous les compartiments S3 que possède le compte. Si vous réactivez ensuite la découverte automatique pour le compte, Macie recommence à inclure les buckets.

Déterminer les types de données sensibles à détecter et à signaler

Par défaut, Macie inspecte les objets S3 à l'aide de l'ensemble d'identifiants de données gérés que nous recommandons pour la découverte automatique des données sensibles. Pour obtenir la liste de ces identifiants de données gérés, consultezParamètres par défaut pour la découverte automatique des données sensibles.

Vous pouvez adapter les analyses pour qu'elles se concentrent sur des types spécifiques de données sensibles. Pour ce faire, modifiez les paramètres de découverte automatique des données sensibles de votre compte de l'une des manières suivantes :

- Ajouter ou supprimer des identifiants de données gérées — Un identifiant de données gérées est un ensemble de critères et de techniques intégrés conçus pour détecter un type spécifique de données sensibles, telles que les numéros de carte de crédit, les clés d'accès AWS secrètes ou les numéros de passeport d'un pays ou d'une région en particulier. Pour plus d'informations, consultez Utilisation des identificateurs de données gérés.
- Ajouter ou supprimer des identifiants de données personnalisés : un identifiant de données personnalisé est un ensemble de critères que vous définissez pour détecter les données sensibles. Grâce aux identificateurs de données personnalisés, vous pouvez détecter les données sensibles qui reflètent les scénarios particuliers de votre organisation, la propriété intellectuelle ou les données propriétaires, telles que les identifiants des employés, les numéros

de compte client ou les classifications de données internes. Pour plus d'informations, consultez Création d'identificateurs de données personnalisés.

- Ajouter ou supprimer des listes d'autorisation : dans Macie, une liste d'autorisation indique le texte ou un modèle de texte que vous souhaitez que Macie ignore dans les objets S3. Il s'agit généralement d'exceptions relatives aux données sensibles propres à vos scénarios ou à votre environnement particuliers, telles que les noms publics ou les numéros de téléphone de votre organisation, ou des exemples de données que votre organisation utilise à des fins de test. Pour plus d'informations, consultez Définition des exceptions relatives aux données sensibles à l'aide de listes d'autorisation.

Si vous modifiez les paramètres, Macie les applique au début du cycle d'analyse quotidien suivant. Si vous êtes l'administrateur Macie d'une organisation, Macie utilise les paramètres de votre compte lorsqu'il analyse les objets S3 pour d'autres comptes de votre organisation.

Vous pouvez également ajuster les paramètres au niveau du compartiment afin de déterminer si des types spécifiques de données sensibles sont inclus dans les évaluations de la sensibilité d'un compartiment. Pour savoir comment procéder, veuillez consulter la section Gestion de la découverte automatisée des données sensibles pour des compartiments S3 individuels.

Calcul des scores de sensibilité

Par défaut, Macie calcule automatiquement un score de sensibilité pour chaque compartiment S3 à usage général qu'il surveille et analyse pour votre compte. Si vous êtes l'administrateur Macie d'une organisation, cela inclut les compartiments que possèdent vos comptes membres.

Dans Macie, un score de sensibilité est une mesure quantitative de l'intersection de deux dimensions principales : la quantité de données sensibles que Macie a trouvées dans un bucket et la quantité de données que Macie a analysées dans un bucket. Le score de sensibilité d'un seau détermine l'étiquette de sensibilité que Macie attribue au seau. Une étiquette de sensibilité est une représentation qualitative du score de sensibilité d'un compartiment, par exemple, Sensible, Non sensible et Pas encore analysé. Pour plus de détails sur la plage de scores de sensibilité et d'étiquettes définie par Macie, voirNotation de sensibilité pour les compartiments S3.

> **Important**
>
> Le score de sensibilité et l'étiquette d'un compartiment S3 n'impliquent ni n'indiquent le caractère critique ou l'importance que le compartiment ou les objets du compartiment peuvent avoir pour votre organisation. Ils sont plutôt destinés à fournir des points de

référence qui peuvent vous aider à identifier et à surveiller les risques de sécurité potentiels.

Lorsque vous activez initialement la découverte automatique des données sensibles, Macie attribue automatiquement un score de sensibilité de 50 et l'étiquette Pas encore analysé à chaque compartiment S3. L'exception concerne les seaux vides. Un bucket vide est un bucket qui ne stocke aucun objet ou qui ne contient aucun (0) octet de données. Si tel est le cas pour un compartiment, Macie attribue un score de 1 au compartiment et lui attribue l'étiquette Non sensible.

À mesure que la découverte automatique des données sensibles progresse, Macie met à jour les scores de sensibilité et les étiquettes pour refléter les résultats des analyses. Par exemple :

- Si Macie ne trouve aucune donnée sensible dans un objet, Macie diminue le score de sensibilité du compartiment et met à jour l'étiquette de sensibilité du compartiment si nécessaire.
- Si Macie trouve des données sensibles dans un objet, Macie augmente le score de sensibilité du compartiment et met à jour l'étiquette de sensibilité du compartiment si nécessaire.
- Si Macie trouve des données sensibles dans un objet qui est ensuite modifié, Macie supprime les données sensibles détectées pour l'objet du score de sensibilité du compartiment et met à jour l'étiquette de sensibilité du compartiment si nécessaire.
- Si Macie trouve des données sensibles dans un objet qui est ensuite supprimé, Macie supprime les données sensibles détectées pour l'objet du score de sensibilité du compartiment et met à jour l'étiquette de sensibilité du compartiment si nécessaire.

Vous pouvez ajuster les paramètres de notation de sensibilité pour des compartiments S3 individuels en incluant ou en excluant des types spécifiques de données sensibles du score d'un compartiment. Vous pouvez également annuler le score calculé d'un compartiment en attribuant manuellement le score maximum (100) au compartiment. Si vous attribuez le score maximum, le compartiment est étiqueté Sensible. Pour plus d'informations, consultez Gestion de la découverte automatique pour des compartiments S3 individuels.

Génération de métadonnées, de statistiques et de résultats

Lorsque vous activez la découverte automatique des données sensibles, Macie génère et commence à gérer des données d'inventaire, des statistiques et d'autres informations supplémentaires sur les compartiments à usage général S3 qu'il surveille et analyse pour votre compte. Si vous êtes l'administrateur Macie d'une organisation, cela inclut par défaut les compartiments que possèdent vos comptes membres.

Les informations supplémentaires capturent les résultats des activités automatisées de découverte de données sensibles effectuées par Macie jusqu'à présent. Elle complète également les autres informations fournies par Macie concernant vos données Amazon S3, telles que les paramètres d'accès public et d'accès partagé pour les compartiments individuels. Les informations supplémentaires incluent :

- Statistiques agrégées sur la sensibilité des données, telles que le nombre total de compartiments dans lesquels Macie a trouvé des données sensibles et le nombre de ces compartiments accessibles au public.
- Une représentation visuelle interactive de la sensibilité des données dans l'ensemble de votre parc de données Amazon S3.
- Informations détaillées au niveau du compartiment indiquant l'état actuel des analyses. Par exemple, une liste des objets que Macie a analysés dans un compartiment, les types de données sensibles que Macie a trouvés dans un compartiment et le nombre d'occurrences de chaque type de données sensibles trouvées par Macie.

Les informations incluent également des statistiques et des informations qui peuvent vous aider à évaluer et à surveiller la couverture de vos données Amazon S3. Vous pouvez vérifier l'état des analyses pour l'ensemble de votre parc de données et pour les compartiments S3 individuels de votre inventaire de compartiments. Vous pouvez également identifier les problèmes qui empêchaient Macie d'analyser des objets dans des compartiments spécifiques. Si vous corrigez les problèmes, vous pouvez augmenter la couverture de vos données Amazon S3 lors des cycles d'analyse suivants. Pour plus d'informations, consultez Évaluation de la couverture de la découverte automatique des données sensibles.

Macie recalcule et met à jour automatiquement ces informations pendant qu'il effectue la découverte automatique des données sensibles. Par exemple, si Macie trouve des données sensibles dans un objet S3 qui est ensuite modifié ou supprimé, Macie met à jour les métadonnées du compartiment applicable : supprime l'objet de la liste des objets analysés ; supprime les occurrences de données sensibles trouvées par Macie dans l'objet ; recalcule le score de sensibilité, s'il est calculé automatiquement ; et met à jour l'étiquette de sensibilité si nécessaire pour refléter le nouveau score.

Outre les métadonnées et les statistiques, Macie produit des enregistrements des données sensibles qu'elle trouve et des analyses qu'elle effectue : les résultats de données sensibles, qui signalent les données sensibles trouvées par Macie dans des objets S3 individuels, et les résultats de découverte de données sensibles, qui enregistrent les détails de l'analyse des objets S3 individuels.

Pour plus d'informations, consultez Examen des statistiques et des résultats de découverte automatique de données sensibles.

Considérations

Lorsque vous configurez et utilisez Amazon Macie pour effectuer une découverte automatique des données sensibles relatives à vos données Amazon S3, gardez à l'esprit les points suivants :

- Vos paramètres de découverte automatique s'appliquent uniquement aux paramètres actuels Région AWS. Par conséquent, les analyses et les données qui en résultent ne s'appliquent qu'aux compartiments et objets à usage général S3 de la région actuelle. Pour effectuer une découverte automatique et accéder aux données obtenues dans des régions supplémentaires, activez et configurez la découverte automatique dans chaque région supplémentaire.
- Si vous êtes l'administrateur Macie d'une organisation :
  - Vous pouvez effectuer une découverte automatique pour un compte membre uniquement si Macie est activé pour le compte dans la région actuelle. En outre, vous devez activer la découverte automatique du compte dans cette région. Les membres ne peuvent pas activer la découverte automatique pour leurs propres comptes.
  - Si vous activez la découverte automatique pour un compte membre, Macie utilise les paramètres de découverte automatique de votre compte administrateur lorsqu'elle analyse les données du compte membre. Les paramètres applicables sont les suivants : la liste des compartiments S3 à exclure des analyses, ainsi que les identifiants de données gérés, les identifiants de données personnalisés et les listes d'autorisation à utiliser lors de l'analyse des objets S3. Les membres ne peuvent pas configurer ces paramètres pour leurs propres comptes.
  - Les membres ne peuvent pas accéder aux paramètres de découverte automatique pour leurs compartiments S3. Par exemple, un membre ne peut pas ajuster les paramètres de score de sensibilité d'un bucket dont il est propriétaire. Seul l'administrateur Macie peut accéder à ces paramètres.
  - Les membres ne peuvent pas accéder aux statistiques de découverte de données sensibles et aux autres résultats que Macie fournit directement à leurs compartiments S3. Par exemple, un membre ne peut pas utiliser Macie pour examiner les scores de sensibilité de ses compartiments S3 ou accéder aux résultats produits par la découverte automatique pour ses objets S3. Seul l'administrateur de Macie peut accéder à ces données à l'aide de Macie.
- Si les paramètres d'autorisation d'un compartiment S3 empêchent Macie de récupérer des informations sur le compartiment ou les objets du compartiment ou d'y accéder, Macie ne peut pas effectuer de découverte automatique pour le compartiment. Macie ne peut fournir qu'un sous-

ensemble d'informations sur le bucket, telles que l'ID de compte du propriétaire du Compte AWS bucket, le nom du bucket et la date à laquelle Macie a récemment récupéré les métadonnées du bucket et de l'objet pour le bucket dans le cadre du cycle d'actualisation quotidien. Dans votre inventaire de compartiments, le score de sensibilité de ces compartiments est de 50 et leur étiquette de sensibilité n'a pas encore été analysée.

Pour identifier rapidement les compartiments S3 dans ce cas, reportez-vous aux données de couverture de vos découvertes automatisées. Pour plus d'informations, consultez Évaluation de la couverture de la découverte automatique des données sensibles. Pour étudier le problème lié à un compartiment en particulier, consultez la politique et les paramètres d'autorisation du compartiment dans Amazon S3. Par exemple, le compartiment peut avoir une politique de compartiment restrictive. Pour plus d'informations, consultez Autoriser Macie à accéder aux compartiments et aux objets S3.

- Pour être éligible à la sélection et à l'analyse, un objet S3 doit être stocké dans un compartiment à usage général et doit être classifiable. Un objet classifiable utilise une classe de stockage Amazon S3 prise en charge et possède une extension de nom de fichier pour un format de fichier ou de stockage pris en charge. Pour plus d'informations, consultez Classes et formats de stockage pris en charge.
- Si un objet S3 est chiffré, Macie ne peut l'analyser que s'il est chiffré avec une clé à laquelle Macie peut accéder et est autorisée à utiliser. Pour plus d'informations, consultez Analyse des objets S3 chiffrés. Pour identifier les cas où les paramètres de chiffrement empêchaient Macie d'analyser un ou plusieurs objets d'un compartiment, reportez-vous aux données de couverture de vos découvertes automatisées. Pour plus d'informations, voir Évaluation de la couverture de la découverte automatique des données sensibles.

Configuration de la découverte automatique des données sensibles

Grâce à la découverte automatique des données sensibles, Amazon Macie sélectionne en permanence des échantillons d'objets dans vos compartiments à usage général Amazon Simple Storage Service (Amazon S3) et analyse les objets pour déterminer s'ils contiennent des données sensibles. Si vous êtes l'administrateur Macie d'une organisation, cela inclut par défaut les objets des compartiments S3 détenus par vos comptes membres. Au fur et à mesure que les analyses progressent, Macie met à jour les statistiques, les données d'inventaire et les autres informations qu'il fournit sur vos données Amazon S3. Macie produit également des enregistrements des données sensibles qu'il trouve et des analyses qu'il effectue.

Pour configurer et gérer la découverte automatique des données sensibles, votre compte doit être le compte administrateur Macie d'une organisation ou un compte Macie autonome. Si votre compte fait partie d'une organisation, seul l'administrateur Macie de votre organisation peut activer ou désactiver la découverte automatique des données sensibles pour les comptes de votre organisation. En outre, seul l'administrateur Macie peut configurer les paramètres de découverte automatique des données sensibles pour les comptes. Si vous avez un compte membre et que vous souhaitez que Macie effectue la découverte automatique des données sensibles pour vos compartiments S3, contactez votre administrateur Macie.

Rubriques

Lorsque vous activez, configurez ou désactivez la découverte automatique des données sensibles, vos modifications s'appliquent uniquement aux données actuelles Région AWS. Pour apporter les mêmes modifications dans d'autres régions, répétez les étapes applicables dans chaque région supplémentaire.

Avant de commencer

Avant d'activer ou de configurer la découverte automatique des données sensibles, effectuez les tâches suivantes pour vous assurer que vous disposez des ressources et des autorisations dont vous avez besoin.

Tâches

Ces tâches sont facultatives si vous avez déjà activé et configuré la découverte automatique des données sensibles et que vous souhaitez uniquement modifier les paramètres ou la désactiver.

Configuration d'un référentiel pour les résultats de découverte de données sensibles

Lorsqu'Amazon Macie effectue une découverte automatique de données sensibles, il crée un enregistrement d'analyse pour chaque objet Amazon Simple Storage Service (Amazon S3) sélectionné pour analyse. Ces enregistrements, appelés résultats de découverte de données sensibles, enregistrent les détails de l'analyse des objets S3 individuels. Cela inclut les objets dans lesquels Macie ne trouve pas de données sensibles et les objets que Macie ne peut pas analyser en raison d'erreurs ou de problèmes tels que les paramètres des autorisations. Si Macie trouve des données sensibles dans un objet, le résultat de la découverte de données sensibles inclut des informations sur les données sensibles trouvées par Macie. Les résultats de découverte de données sensibles vous fournissent des enregistrements d'analyse qui peuvent être utiles pour les audits ou les enquêtes sur la confidentialité et la protection des données.

Macie conserve les résultats de la découverte de vos données sensibles pendant 90 jours seulement. Pour accéder aux résultats et permettre leur stockage et leur conservation à long terme, configurez Macie pour qu'il les stocke dans un compartiment S3. Le bucket peut servir de référentiel définitif à long terme pour tous vos résultats de découverte de données sensibles.

Pour vérifier que vous avez configuré ce référentiel, choisissez Discovery results dans le volet de navigation de la console Amazon Macie. Si vous préférez le faire par programmation, utilisez le GetClassificationExportConfigurationfonctionnement de l'API Amazon Macie. Pour en savoir plus sur les résultats de découverte de données sensibles et sur la façon de configurer ce référentiel, consultezStockage et conservation des résultats de découverte de données sensibles.

Si vous avez configuré le référentiel, Macie crée un dossier nommé `automated-sensitive-data-discovery` dans le référentiel lorsque vous activez la découverte automatique de données sensibles pour la première fois. Ce dossier contient les résultats de découverte de données sensibles créés par Macie lors de la découverte automatique pour votre compte ou votre organisation.

Vérifiez vos autorisations

Pour vérifier vos autorisations, utilisez AWS Identity and Access Management (IAM) pour examiner les politiques IAM associées à votre identité IAM. Comparez ensuite les informations contenues dans ces politiques à la liste suivante des actions que vous devez être autorisé à effectuer :

- `macie2:GetMacieSession`
- `macie2:UpdateAutomatedDiscoveryConfiguration`
- `macie2:ListClassificationScopes`

- `macie2:UpdateClassificationScope`
- `macie2:ListSensitivityInspectionTemplates`
- `macie2:UpdateSensitivityInspectionTemplate`

La première action vous permet d'accéder à votre compte Amazon Macie. La deuxième action vous permet d'activer ou de désactiver la découverte automatique des données sensibles pour votre compte ou votre organisation. Pour une organisation, cela vous permet également d'activer automatiquement la découverte automatique des données sensibles pour les comptes de votre organisation. Les actions restantes vous permettent d'identifier et de modifier les paramètres de configuration.

Si vous prévoyez d'utiliser la console Amazon Macie pour vérifier ou modifier les paramètres de configuration, vérifiez également que vous êtes autorisé à effectuer les actions suivantes :

- `macie2:GetAutomatedDiscoveryConfiguration`
- `macie2:GetClassificationScope`
- `macie2:GetSensitivityInspectionTemplate`

Ces actions vous permettent de récupérer vos paramètres de configuration actuels et l'état de la découverte automatique des données sensibles pour votre compte ou votre organisation. L'autorisation d'effectuer ces actions est facultative si vous envisagez de modifier les paramètres de configuration par programmation.

Si vous êtes l'administrateur Macie d'une organisation, vous devez également être autorisé à effectuer les actions suivantes :

- `macie2:ListAutomatedDiscoveryAccounts`
- `macie2:BatchUpdateAutomatedDiscoveryAccounts`

La première action vous permet de récupérer l'état de la découverte automatique des données sensibles pour les comptes individuels de votre organisation. La deuxième action vous permet d'activer ou de désactiver la découverte automatique des données sensibles pour les comptes individuels de votre organisation.

Si vous n'êtes pas autorisé à effectuer les actions requises, demandez de l'aide à votre AWS administrateur.

Options de configuration pour les organisations

Si un compte fait partie d'une organisation qui gère de manière centralisée plusieurs comptes Amazon Macie, l'administrateur Macie de l'organisation configure et gère la découverte automatique des données sensibles pour les comptes de l'organisation. Cela inclut les paramètres qui définissent la portée et la nature des analyses effectuées par Macie pour les comptes. Les membres ne peuvent pas accéder à ces paramètres pour leurs propres comptes.

Si vous êtes l'administrateur Macie d'une organisation, vous pouvez définir la portée des analyses de plusieurs manières :

- Activer automatiquement la découverte automatique des données sensibles pour les comptes : lorsque vous activez la découverte automatique des données sensibles, vous spécifiez si vous souhaitez l'activer automatiquement pour tous les comptes existants et les nouveaux comptes membres, uniquement pour les nouveaux comptes membres ou aucun compte. Si vous l'activez automatiquement pour les nouveaux comptes membres, elle est activée pour tout compte qui rejoint ultérieurement votre organisation, lorsque le compte rejoint votre organisation dans Macie. S'il est activé pour un compte, Macie inclut les compartiments S3 détenus par le compte. Si elle est désactivée pour un compte, Macie exclut les buckets détenus par le compte.
- Activez de manière sélective la découverte automatique des données sensibles pour les comptes : avec cette option, vous activez ou désactivez la découverte automatique des données sensibles pour les comptes individuels sur une case-by-case base individuelle. Si vous l'activez pour un compte, Macie inclut les compartiments S3 détenus par le compte. Si vous ne l'activez pas ou si vous le désactivez pour un compte, Macie exclut les buckets détenus par le compte.
- Exclure des compartiments S3 spécifiques de la découverte automatique des données sensibles — Si vous activez la découverte automatique des données sensibles pour un ou plusieurs comptes, vous pouvez exclure des compartiments S3 spécifiques détenus par les comptes. Macie ignore ensuite les compartiments lorsqu'il effectue une découverte automatique pour votre organisation. Pour exclure des compartiments particuliers, ajoutez-les à la liste d'exclusion des compartiments dans les paramètres de configuration de votre compte administrateur. Vous pouvez exclure jusqu'à 1 000 compartiments pour votre organisation.

Par défaut, la découverte automatique des données sensibles est activée automatiquement pour tous les comptes nouveaux et existants d'une organisation. De plus, Macie inclut tous les compartiments S3 que possèdent les comptes. Si vous conservez les paramètres par défaut, Macie effectue une découverte automatique de tous les compartiments qu'il surveille et analyse pour votre compte administrateur, y compris tous les compartiments que possèdent vos comptes membres.

En tant qu'administrateur Macie, vous définissez également la nature des analyses que Macie effectue pour votre organisation. Pour ce faire, configurez des paramètres supplémentaires pour votre compte administrateur : les identifiants de données gérés, les identifiants de données personnalisés et les listes d'autorisations que vous souhaitez que Macie utilise lorsqu'il analyse des objets S3. Macie utilise les paramètres de votre compte administrateur lorsqu'il analyse les objets S3 pour d'autres comptes de votre organisation.

Permettre la découverte automatique des données sensibles

Lorsque vous activez la découverte automatique des données sensibles, Amazon Macie commence à évaluer vos données d'inventaire Amazon S3 et à effectuer d'autres activités de découverte automatique pour votre compte en cours. Région AWS Si vous êtes l'administrateur Macie d'une organisation, cela inclut par défaut les compartiments S3 que possèdent vos comptes membres. En fonction de la taille de votre parc de données Amazon S3, les statistiques de découverte de données sensibles et d'autres résultats peuvent commencer à apparaître dans les 48 heures.

Pour activer la découverte automatique des données sensibles pour un compte ou une organisation, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie. Pour l'activer à l'aide de la console, procédez comme suit. Pour l'activer par programmation, utilisez les opérations suivantes de l'API Amazon Macie BatchUpdateAutomatedDiscoveryAccounts: pour les comptes individuels d'une organisation, UpdateAutomatedDiscoveryConfigurationou, pour une organisation, un compte administrateur Macie ou un compte Macie autonome.

Pour permettre la découverte automatique des données sensibles

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez activer la découverte automatique des données sensibles.
3. Dans le volet de navigation, sous Paramètres, choisissez Découverte automatisée des données sensibles.
4. Si vous avez un compte Macie autonome, choisissez Activer dans la section État.
5. Si vous êtes l'administrateur Macie d'une organisation, choisissez une option dans la section État pour spécifier les comptes permettant la découverte automatique des données sensibles pour :

   - Pour l'activer pour tous les comptes de votre organisation, choisissez Activer. Dans la boîte de dialogue qui apparaît, sélectionnez Mon organisation. Pour l'activer également automatiquement pour les comptes qui rejoignent ultérieurement votre organisation,

sélectionnez Activer automatiquement pour les nouveaux comptes. Lorsque vous avez terminé, choisissez Activer.

- Pour l'activer uniquement pour certains comptes de membres, choisissez Gérer les comptes. Ensuite, dans le tableau de la page Comptes, cochez la case correspondant à chaque compte pour lequel vous souhaitez l'activer. Lorsque vous avez terminé, choisissez Activer la découverte automatique des données sensibles dans le menu Actions.
- Pour l'activer uniquement pour votre compte administrateur Macie, choisissez Activer. Dans la boîte de dialogue qui apparaît, choisissez Mon compte et désactivez Activer automatiquement pour les nouveaux comptes. Lorsque vous avez terminé, choisissez Activer.

Pour vérifier ou modifier ultérieurement le statut de la découverte automatique des données sensibles pour les comptes individuels de votre organisation, sélectionnez Comptes dans le volet de navigation. Sur la page Comptes, le champ Découverte automatique des données sensibles du tableau indique l'état actuel de la découverte automatique d'un compte. Pour modifier le statut d'un compte, sélectionnez le compte, puis utilisez le menu Actions pour activer la désactivation de la découverte automatique pour le compte.

Après avoir activé la découverte automatique des données sensibles, passez en revue et configurez vos paramètres pour affiner les analyses effectuées par Macie.

Configuration des paramètres de découverte automatique des données sensibles

Si vous activez la découverte automatique des données sensibles pour votre compte ou votre organisation, vous pouvez ajuster vos paramètres de découverte automatique pour affiner les analyses effectuées par Amazon Macie. Ces paramètres spécifient les compartiments S3 à exclure des analyses. Ils spécifient également les types et les occurrences de données sensibles à détecter et à signaler : les identifiants de données gérés, les identifiants de données personnalisés et les listes d'autorisations à utiliser lors de l'analyse des objets S3.

Par défaut, Macie effectue la découverte automatique des données sensibles pour tous les compartiments S3 à usage général qu'il surveille et analyse pour votre compte. Si vous êtes l'administrateur Macie d'une organisation, cela inclut les compartiments que possèdent vos comptes membres. Vous pouvez exclure des compartiments spécifiques des analyses. Par exemple, vous pouvez exclure les compartiments qui stockent généralement des données de AWS journalisation, telles que les journaux AWS CloudTrail d'événements. Si vous excluez un bucket, vous pouvez ensuite l'inclure à nouveau.

En outre, Macie analyse les objets S3 en utilisant uniquement l'ensemble d'identifiants de données gérés que nous recommandons pour la découverte automatique des données sensibles. Macie n'utilise pas d'identificateurs de données personnalisés et n'autorise pas les listes que vous avez définies. Pour personnaliser les analyses, vous pouvez configurer Macie pour qu'il utilise des identifiants de données gérés spécifiques, des identifiants de données personnalisés et des listes d'autorisations.

Les sections suivantes fournissent des informations supplémentaires sur chaque type de paramètre. Ils expliquent également comment modifier un paramètre à l'aide de la console Amazon Macie. Choisissez une section pour en savoir plus. Pour revoir ou modifier les paramètres par programmation, vous pouvez utiliser les opérations suivantes de l'API Amazon Macie UpdateClassificationScope: pour spécifier les compartiments S3 à exclure des analyses, UpdateSensitivityInspectionTemplateet pour spécifier les identifiants de données gérés, les identifiants de données personnalisés et les listes d'autorisation à utiliser.

Si vous modifiez un paramètre, Macie applique votre modification au début du cycle d'évaluation et d'analyse suivant pour la découverte automatique des données sensibles, généralement dans les 24 heures.

Exclure ou inclure les compartiments S3

Par défaut, Macie effectue la découverte automatique des données sensibles pour tous les compartiments S3 à usage général qu'il surveille et analyse pour votre compte. Si vous êtes l'administrateur Macie d'une organisation, cela inclut les compartiments que possèdent vos comptes membres.

Pour affiner la portée, vous pouvez exclure jusqu'à 1 000 compartiments S3 des analyses. Si vous excluez un compartiment, Macie arrête de sélectionner et d'analyser les objets qu'il contient lorsqu'il effectue la découverte automatique de données sensibles. Les statistiques existantes relatives à la découverte de données sensibles et les détails relatifs au compartiment sont conservés. Par exemple, le score de sensibilité actuel du compartiment reste inchangé. Après avoir exclu un bucket, vous pouvez l'inclure à nouveau.

Pour exclure ou inclure des compartiments S3 spécifiques

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez exclure ou inclure des compartiments S3 spécifiques dans les analyses de découverte automatisées.

3. Dans le volet de navigation, sous Paramètres, choisissez Découverte automatisée des données sensibles.

   La page Découverte automatique des données sensibles apparaît et affiche vos paramètres actuels. Sur cette page, la section des compartiments S3 répertorie les compartiments S3 actuellement exclus ou indique que tous les compartiments sont actuellement inclus.
4. Dans la section compartiments S3, choisissez Modifier.
5. Effectuez l'une des actions suivantes :

   - Pour exclure un ou plusieurs compartiments S3, choisissez Ajouter des compartiments à la liste d'exclusion. Ensuite, dans le tableau des compartiments S3, cochez la case correspondant à chaque compartiment que vous souhaitez exclure. Le tableau répertorie tous les compartiments à usage général pour votre compte ou votre organisation dans la région actuelle.
   - Pour inclure un ou plusieurs compartiments S3 que vous avez précédemment exclus, choisissez Supprimer les compartiments de la liste d'exclusion. Ensuite, dans le tableau des compartiments S3, cochez la case correspondant à chaque compartiment que vous souhaitez inclure. Le tableau répertorie tous les compartiments actuellement exclus des analyses de découverte automatisées.

   Pour trouver plus facilement des compartiments spécifiques, entrez des critères de recherche dans le champ de recherche situé au-dessus du tableau. Vous pouvez également trier le tableau en choisissant un titre de colonne.
6. Lorsque vous avez fini de sélectionner des compartiments, choisissez Ajouter ou Supprimer, selon l'option que vous avez choisie à l'étape précédente.

Ajouter ou supprimer des identifiants de données gérées

Un identifiant de données géré est un ensemble de critères et de techniques intégrés conçus pour détecter un type spécifique de données sensibles, par exemple les numéros de carte de crédit, les clés d'accès AWS secrètes ou les numéros de passeport d'un pays ou d'une région en particulier. Par défaut, Macie analyse les objets S3 à l'aide de l'ensemble d'identifiants de données gérés que nous recommandons pour la découverte automatique des données sensibles. Pour consulter la liste de ces identifiants, consultezParamètres par défaut pour la découverte automatique des données sensibles.

Vous pouvez adapter les analyses pour qu'elles se concentrent sur des types spécifiques de données sensibles :

- Ajoutez des identifiants de données gérés pour les types de données sensibles que vous souhaitez que Macie détecte et signale, et
- Supprimez les identifiants de données gérées pour les types de données sensibles que vous ne souhaitez pas que Macie détecte et signale.

Si vous supprimez un identifiant de données gérées, votre modification n'affectera pas les statistiques de découverte de données sensibles existantes ni les détails relatifs aux compartiments S3. Par exemple, si vous supprimez l'identifiant des données gérées pour les clés d'accès AWS secrètes et que Macie a déjà détecté ce type de données dans un bucket, Macie continue de signaler ces détections pour le bucket.

> **Tip**
>
> Au lieu de supprimer un identifiant de données géré, qui affecte les analyses ultérieures de tous les compartiments S3, vous pouvez exclure ses détections des scores de sensibilité pour des compartiments particuliers. Pour plus d'informations, consultez Gestion de la découverte automatisée des données sensibles pour des compartiments S3 individuels.

Pour ajouter ou supprimer des identifiants de données gérées

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez ajouter ou supprimer des identifiants de données gérés dans les analyses de découverte automatisées.
3. Dans le volet de navigation, sous Paramètres, choisissez Découverte automatisée des données sensibles.

   La page Découverte automatique des données sensibles apparaît et affiche vos paramètres actuels. Sur cette page, la section Identifiants de données gérés affiche vos paramètres actuels, organisés en deux onglets :

- Ajouté par défaut : cet onglet répertorie les identifiants de données gérées que vous avez ajoutés. Macie utilise ces identifiants en plus de ceux qui sont définis par défaut et que vous n'avez pas supprimés.
- Supprimé par défaut : cet onglet répertorie les identifiants de données gérées que vous avez supprimés. Macie n'utilise pas ces identifiants.

4. Dans la section Identifiants de données gérés, choisissez Modifier.
5. Effectuez l'une des actions suivantes :

   - Pour ajouter un ou plusieurs identifiants de données gérées, cliquez sur l'onglet Ajouté par défaut. Dans le tableau, cochez ensuite la case correspondant à chaque identifiant de données gérées à ajouter. Si une case à cocher est déjà sélectionnée, vous avez déjà ajouté cet identifiant.
   - Pour supprimer un ou plusieurs identifiants de données gérés, sélectionnez l'onglet Supprimé par défaut. Dans le tableau, cochez ensuite la case correspondant à chaque identifiant de données gérées à supprimer. Si une case est déjà cochée, vous avez déjà supprimé cet identifiant.

   Sur chaque onglet, le tableau affiche une liste de tous les identifiants de données gérés actuellement fournis par Macie. Dans le tableau, la première colonne indique l'ID de chaque identifiant de données gérées. L'identifiant décrit le type de données sensibles qu'un identifiant est conçu pour détecter, par exemple, USA_PASSPORT_NUMBER pour les numéros de passeport américains. Pour trouver plus facilement des identifiants de données gérées spécifiques, entrez des critères de recherche dans le champ de recherche situé au-dessus du tableau. Vous pouvez également trier le tableau en choisissant un titre de colonne. Pour plus de détails sur chaque identifiant, consultezUtilisation des identificateurs de données gérés.
6. Lorsque vous avez terminé, choisissez Enregistrer.

Ajouter ou supprimer des identifiants de données personnalisés

Un identificateur de données personnalisé est un ensemble de critères que vous définissez pour détecter les données sensibles. Les critères sont constitués d'une expression régulière (regex) qui définit un modèle de texte à mettre en correspondance et, éventuellement, des séquences de caractères et une règle de proximité qui affinent les résultats. Pour en savoir plus, veuillez consulter la section Création d'identificateurs de données personnalisés.

Par défaut, Amazon Macie n'utilise pas d'identifiants de données personnalisés lorsqu'il effectue la découverte automatique de données sensibles. Si vous souhaitez que Macie utilise des identifiants de données personnalisés spécifiques, vous pouvez les ajouter aux analyses. Macie utilise ensuite les identifiants de données personnalisés en plus des identifiants de données gérés pour lesquels vous configurez Macie.

Si vous ajoutez un identifiant de données personnalisé, vous pouvez le supprimer ultérieurement. Votre modification n'affecte pas les statistiques de découverte de données sensibles existantes ni les détails relatifs aux compartiments S3. En d'autres termes, si vous supprimez un identifiant de données personnalisé qui a précédemment généré des détections pour un bucket, Macie continue de signaler ces détections pour le bucket. Toutefois, au lieu de supprimer l'identifiant, qui affecte les analyses ultérieures de tous les compartiments, envisagez d'exclure ses détections des scores de sensibilité pour des compartiments particuliers uniquement. Pour plus d'informations, consultez Gestion de la découverte automatisée des données sensibles pour des compartiments S3 individuels.

Pour ajouter ou supprimer des identifiants de données personnalisés

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez ajouter ou supprimer des identifiants de données personnalisés dans les analyses de découverte automatisées.
3. Dans le volet de navigation, sous Paramètres, choisissez Découverte automatisée des données sensibles.

   La page Découverte automatique des données sensibles apparaît et affiche vos paramètres actuels. Sur cette page, la section Identifiants de données personnalisés répertorie les identifiants de données personnalisés que vous avez ajoutés ou indique que vous n'avez sélectionné aucun identifiant de données personnalisé.
4. Dans la section Identifiants de données personnalisés, choisissez Modifier.
5. Effectuez l'une des actions suivantes :

   - Pour ajouter un ou plusieurs identifiants de données personnalisés, cochez la case correspondant à chaque identifiant de données personnalisé à ajouter. Si une case à cocher est déjà sélectionnée, vous avez déjà ajouté cet identifiant.
   - Pour supprimer un ou plusieurs identifiants de données personnalisés, décochez la case correspondant à chaque identifiant de données personnalisé à supprimer. Si une case est déjà décochée, Macie n'utilise pas cet identifiant actuellement.

> **Tip**
>
> Pour vérifier ou tester les paramètres d'un identifiant de données personnalisé avant de l'ajouter ou de le supprimer, cliquez sur l'icône de lien ( ) à côté du nom de l'identifiant. Macie ouvre une page qui affiche les paramètres de l'identifiant. Pour tester également l'identifiant avec des exemples de données, entrez jusqu'à 1 000 caractères de texte dans la zone Exemple de données de cette page. Choisissez ensuite Test. Macie évalue les échantillons de données et indique le nombre de correspondances.

6. Lorsque vous avez terminé, choisissez Enregistrer.

Ajouter ou supprimer des listes d'autorisation

Dans Amazon Macie, une liste d'autorisation définit un texte spécifique ou un modèle de texte que vous souhaitez que Macie ignore lorsqu'il inspecte les objets S3 pour détecter la présence de données sensibles. Si le texte correspond à une entrée ou à un modèle d'une liste d'autorisation, Macie ne le signale pas. C'est le cas même si le texte correspond aux critères d'un identifiant de données géré ou personnalisé. Pour en savoir plus, veuillez consulter la section Définition des exceptions relatives aux données sensibles à l'aide de listes d'autorisation.

Par défaut, Macie n'utilise pas de listes d'autorisation lorsqu'il effectue la découverte automatique de données sensibles. Si vous souhaitez que Macie utilise des listes d'autorisations spécifiques, vous pouvez les ajouter aux analyses. Si vous ajoutez une liste d'autorisations, vous pouvez ensuite la supprimer.

Pour ajouter ou supprimer des listes d'autorisation

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez ajouter ou supprimer des listes d'autorisation dans les analyses de découverte automatisées.
3. Dans le volet de navigation, sous Paramètres, choisissez Découverte automatisée des données sensibles.

La page Découverte automatique des données sensibles apparaît et affiche vos paramètres actuels. Sur cette page, la section Listes autorisées indique les listes autorisées que vous avez déjà ajoutées ou indique que vous n'avez sélectionné aucune liste d'autorisation.

4. Dans la section Autoriser les listes, choisissez Modifier.
5. Effectuez l'une des actions suivantes :

   - Pour ajouter une ou plusieurs listes d'autorisations, cochez la case correspondant à chaque liste d'autorisation à ajouter. Si une case à cocher est déjà sélectionnée, vous avez déjà ajouté cette liste.
   - Pour supprimer une ou plusieurs listes d'autorisations, décochez la case correspondant à chaque liste d'autorisation à supprimer. Si une case est déjà décochée, Macie n'utilise pas cette liste actuellement.

   > **Tip**
   >
   > Pour vérifier les paramètres d'une liste d'autorisation avant de l'ajouter ou de la supprimer, cliquez sur l'icône de lien () à côté du nom de la liste. Macie ouvre une page qui affiche les paramètres de la liste. Si la liste indique une expression régulière (regex), vous pouvez également utiliser cette page pour tester l'expression régulière avec des exemples de données. Pour ce faire, entrez jusqu'à 1 000 caractères de texte dans la zone Exemple de données, puis choisissez Test. Macie évalue les échantillons de données et indique le nombre de correspondances.

6. Lorsque vous avez terminé, choisissez Enregistrer.

Désactivation de la découverte automatique des données sensibles

Vous pouvez désactiver la découverte automatique des données sensibles pour un compte ou une organisation à tout moment. Dans ce cas, Macie arrête d'effectuer toutes les activités de découverte automatique pour le compte ou l'organisation avant le début d'un cycle d'évaluation et d'analyse ultérieur, généralement dans les 48 heures. Les effets supplémentaires varient :

- Si vous le désactivez pour un compte de votre organisation, vous pouvez continuer à accéder à toutes les données statistiques, aux données d'inventaire et aux autres informations produites et

fournies directement par Macie tout en effectuant la découverte automatique du compte. Vous pouvez également réactiver la découverte automatique du compte. Macie reprend ensuite toutes les activités de découverte automatisées pour le compte.

- Si vous le désactivez pour votre organisation ou pour un compte Macie autonome, vous perdez l'accès à toutes les données statistiques, aux données d'inventaire et aux autres informations produites et fournies directement par Macie lors de la découverte automatique pour votre organisation ou votre compte. Par exemple, votre inventaire de compartiments S3 n'inclut plus de visualisations de sensibilité ni de statistiques d'analyse. Vous pourrez ensuite le réactiver. Macie reprend ensuite toutes les activités de découverte automatisées pour votre organisation ou votre compte. Si vous le réactivez dans les 30 jours, vous retrouverez l'accès à toutes les données et informations que Macie a précédemment produites et fournies directement lors de la découverte automatique. Si vous ne le réactivez pas dans les 30 jours, Macie supprime définitivement ces données et informations.

Vous pouvez continuer à accéder aux résultats de données sensibles produits par Macie tout en effectuant la découverte automatique de données sensibles pour votre organisation ou votre compte. Macie conserve les résultats pendant 90 jours. En outre, les données que vous avez stockées ou publiées auprès d'autres personnes Services AWS restent intactes et ne sont pas affectées, comme les résultats de découverte de données sensibles dans Amazon S3 et les événements de recherche sur Amazon EventBridge.

Pour désactiver la découverte automatique des données sensibles, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie. Pour le désactiver à l'aide de la console, procédez comme suit. Pour le désactiver par programmation, utilisez les opérations suivantes de l'API Amazon Macie BatchUpdateAutomatedDiscoveryAccounts: pour les comptes individuels d'une organisation, UpdateAutomatedDiscoveryConfigurationou, pour une organisation, un compte administrateur Macie ou un compte Macie autonome.

Pour désactiver la découverte automatique des données sensibles

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez désactiver la découverte automatique des données sensibles.
3. Dans le volet de navigation, sous Paramètres, choisissez Découverte automatisée des données sensibles.

4. Si vous êtes l'administrateur Macie d'une organisation, choisissez une option dans la section État pour spécifier les comptes pour lesquels désactiver la découverte automatique des données sensibles pour :

   - Pour le désactiver uniquement pour certains comptes de membres, choisissez Gérer les comptes. Ensuite, dans le tableau de la page Comptes, cochez la case correspondant à chaque compte pour lequel vous souhaitez la désactiver. Lorsque vous avez terminé, choisissez Désactiver la découverte automatique des données sensibles dans le menu Actions.
   - Pour le désactiver uniquement pour votre compte administrateur Macie, choisissez Désactiver. Dans la boîte de dialogue qui apparaît, choisissez Mon compte, puis sélectionnez Désactiver.
   - Pour le désactiver pour tous les comptes de votre organisation et pour l'ensemble de votre organisation, choisissez Désactiver. Dans la boîte de dialogue qui apparaît, choisissez Mon organisation, puis sélectionnez Désactiver.
5. Si vous avez un compte Macie autonome, choisissez Désactiver dans la section État.

Gestion de la découverte automatisée des données sensibles pour des compartiments S3 individuels

Lorsque vous consultez et évaluez les statistiques et les résultats de découverte automatique de données sensibles, vous pouvez ajuster le score de sensibilité et d'autres paramètres pour les compartiments Amazon Simple Storage Service (Amazon S3) individuels. En ajustant ces paramètres, vous pouvez affiner les évaluations de sensibilité de votre parc de données Amazon S3 dans son ensemble et des compartiments spécifiques qu'il contient. Vous pouvez également saisir les résultats des enquêtes que vous effectuez pour des compartiments spécifiques.

Vous pouvez ajuster les paramètres de découverte automatique des données sensibles pour un compartiment S3 de la manière suivante.

Attribuer un score de sensibilité

Par défaut, Amazon Macie calcule automatiquement le score de sensibilité d'un bucket. Le score est basé principalement sur la quantité de données sensibles que Macie a trouvées dans un compartiment et sur la quantité de données que Macie a analysées dans un compartiment. Pour plus d'informations, consultez Notation de sensibilité pour les compartiments S3.

Vous pouvez annuler le score calculé d'un bucket et attribuer manuellement le score maximum (100), qui applique également le label Sensitive au bucket. Dans ce cas, Macie continue à effectuer une découverte automatique pour le bucket. Cependant, les analyses ultérieures n'affectent pas le score du bucket. Pour calculer à nouveau le score automatiquement, modifiez à nouveau le paramètre.

Exclure ou inclure des types de données sensibles spécifiques dans le score de sensibilité

S'il est calculé automatiquement, le score de sensibilité d'un compartiment est basé en partie sur la quantité de données sensibles que Macie a trouvées dans le compartiment. Cela tient principalement à la nature et au nombre de types de données sensibles que Macie a trouvés dans le compartiment et au nombre d'occurrences de chaque type. Par défaut, Macie inclut les occurrences de tous les types de données sensibles lorsqu'il calcule le score de sensibilité d'un bucket.

Vous pouvez ajuster le calcul en excluant ou en incluant des types spécifiques de données sensibles dans le score d'un bucket. Par exemple, si Macie a détecté des adresses postales dans un bucket et que vous déterminez que cela est acceptable, vous pouvez exclure toutes les occurrences d'adresses postales du score du bucket. Si vous excluez un type de données sensibles, Macie continue d'inspecter le compartiment pour détecter ce type de données et de signaler les occurrences détectées. Toutefois, ces occurrences n'affectent pas le score calculé du bucket. Pour inclure à nouveau un type de données sensibles dans le magasin calculé, modifiez à nouveau le paramètre.

Exclure ou inclure le compartiment dans les analyses ultérieures

Par défaut, Macie effectue une découverte automatique pour tous les compartiments à usage général qu'il surveille et analyse pour votre compte. Si vous êtes l'administrateur Macie d'une organisation, les paramètres par défaut incluent les compartiments que possèdent vos comptes membres. Vous pouvez exclure des compartiments spécifiques des analyses. Par exemple, vous pouvez exclure les compartiments qui stockent généralement des données de AWS journalisation, telles que les journaux AWS CloudTrail d'événements.

Si vous excluez un bucket, les statistiques de découverte de données sensibles existantes et les détails relatifs au bucket sont conservés. Par exemple, le score de sensibilité actuel du bucket reste inchangé. Toutefois, Macie arrête d'analyser les objets du compartiment lorsqu'il effectue une découverte automatique. Après avoir exclu un bucket, vous pouvez l'inclure à nouveau.

Si vous modifiez un paramètre qui affecte le score de sensibilité d'un compartiment S3, Macie commence immédiatement à recalculer et à mettre à jour les statistiques et informations pertinentes

qu'il fournit sur vos données Amazon S3. Par exemple, si vous attribuez le score maximum à un bucket, Macie augmente le nombre de buckets sensibles dans les statistiques agrégées de votre compte ou de votre organisation.

Procédez comme suit pour modifier un paramètre à l'aide de la console Amazon Macie. Pour modifier un paramètre par programmation, vous pouvez utiliser les opérations suivantes de l'API Amazon Macie UpdateResourceProfile: pour attribuer un score de sensibilité à un bucket UpdateResourceProfileDetections; pour exclure ou inclure ultérieurement des types de données sensibles dans le score d'un bucket ; et UpdateClassificationScopepour exclure ou inclure un bucket dans les analyses ultérieures.

Pour modifier les paramètres de découverte automatique des données sensibles pour un compartiment S3

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez S3 buckets (Compartiments S3). La page des compartiments S3 affiche l'inventaire de vos compartiments.

   Par défaut, la page n'affiche pas les données relatives aux compartiments actuellement exclus des analyses. Si vous êtes l'administrateur Macie d'une organisation, elle n'affiche pas non plus les données des comptes pour lesquels la découverte automatique des données sensibles est actuellement désactivée. Pour afficher ces données, choisissez X dans le jeton de filtre Est surveillé par détection automatique situé sous le filtre.
3. Choisissez le compartiment S3 dont vous souhaitez modifier les paramètres. Vous pouvez choisir le compartiment à l'aide de la vue tabulaire () ou de la carte interactive ().
4. Dans le panneau de détails, effectuez l'une des opérations suivantes :

   - Pour annuler le score calculé et attribuer manuellement un score de sensibilité au bucket, activez Assigner le score maximum (). Cela fait passer le score du bucket à 100 et applique le label Sensitive au bucket.

Pour attribuer un score que Macie calcule automatiquement, désactivez Attribuer un score maximum
()
.

- Pour exclure le bucket des analyses ultérieures, activez Exclure de la découverte automatique
( ).

  Si vous avez précédemment exclu le compartiment des analyses, désactivez Exclure de la découverte automatique
  ( )
  pour l'inclure à nouveau.
- Pour exclure ou inclure des occurrences de types spécifiques de données sensibles dans le score de sensibilité du bucket, choisissez l'onglet Sensibilité. Dans le tableau des détections, cochez la case correspondant au type de données sensibles à exclure ou à inclure. Ensuite, dans le menu Actions, choisissez Exclure du score pour exclure le type ou choisissez Inclure dans le score pour inclure le type.

  Dans le tableau, le champ Type de données sensibles indique l'identifiant unique (ID) de l'identifiant des données gérées qui a détecté les données, ou le nom de l'identifiant de données personnalisé qui a détecté les données. L'identifiant d'un identifiant de données géré décrit le type de données sensibles que l'identifiant est conçu pour détecter, par exemple, USA_PASSPORT_NUMBER pour les numéros de passeport américains. Pour plus de détails sur chaque identifiant de données gérées, consultezUtilisation des identificateurs de données gérés.

Si vous avez modifié un paramètre qui affecte le score de sensibilité du compartiment S3, Macie commence immédiatement à recalculer et à mettre à jour les statistiques pertinentes relatives à la découverte de données sensibles et les autres informations relatives au compartiment.

Évaluation de la couverture de la découverte automatique des données sensibles

Au fur et à mesure que la découverte automatique des données sensibles progresse pour votre compte ou votre organisation, Amazon Macie fournit des statistiques et des informations pour vous aider à évaluer et à surveiller sa couverture de votre parc de données Amazon Simple Storage Service (Amazon S3). Grâce à ces données, vous pouvez vérifier l'état de la découverte automatique des données sensibles pour l'ensemble de votre parc de données et pour les compartiments S3

individuels de votre inventaire de compartiments. Vous pouvez également identifier les problèmes qui empêchaient Macie d'analyser des objets dans des compartiments spécifiques. Si vous corrigez les problèmes, vous pouvez augmenter la couverture de vos données Amazon S3 lors des cycles d'analyse suivants.

Les données de couverture fournissent un aperçu de l'état actuel de la découverte automatique de données sensibles pour vos compartiments à usage général S3 à l'heure actuelle Région AWS. Si vous êtes l'administrateur Macie d'une organisation, cela inclut les compartiments que possèdent vos comptes membres. Pour chaque compartiment, les données indiquent si des problèmes sont survenus lorsque Macie a tenté d'analyser les objets du compartiment. Si des problèmes sont survenus, les données indiquent la nature de chaque problème et, dans certains cas, le nombre d'incidents. Les données sont mises à jour au fur et à mesure que la découverte automatique des données sensibles progresse chaque jour. Si Macie analyse ou tente d'analyser un ou plusieurs objets d'un compartiment au cours d'un cycle d'analyse quotidien, Macie met à jour la couverture et les autres données pour refléter les résultats.

Pour certains types de problèmes, vous pouvez consulter les données agrégées pour tous vos compartiments S3 à usage général et éventuellement effectuer une analyse détaillée pour obtenir des informations supplémentaires sur chaque compartiment. Par exemple, les données de couverture peuvent vous aider à identifier rapidement tous les compartiments auxquels Macie n'est pas autorisée à accéder pour votre compte. Les données de couverture signalent également les problèmes survenus au niveau de l'objet. Ces problèmes, appelés erreurs de classification, empêchaient Macie d'analyser des objets spécifiques dans un compartiment. Par exemple, vous pouvez déterminer le nombre d'objets que Macie n'a pas pu analyser dans un compartiment parce que les objets sont chiffrés avec une clé AWS Key Management Service (AWS KMS) qui n'est plus disponible.

Si vous utilisez la console Amazon Macie pour consulter les données de couverture, votre consultation des données inclut des conseils pour résoudre chaque type de problème. Les rubriques suivantes de cette section fournissent également des conseils de correction pour chaque type.

Rubriques

- Erreur de classification : clé KMS non valide
- Erreur de classification : autorisation refusée
- Inclassable

Examen des données de couverture relatives à la découverte automatique des données sensibles

Pour examiner et évaluer la couverture de la découverte automatique des données sensibles, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie. La console et l'API fournissent des données qui indiquent l'état actuel des analyses pour vos compartiments à usage général Amazon Simple Storage Service (Amazon S3) dans le contexte actuel. Région AWS Les données incluent des informations sur les problèmes qui créent des lacunes dans les analyses :

- Des compartiments auxquels Macie n'est pas autorisé à accéder. Macie ne peut analyser aucun objet dans ces compartiments car les paramètres d'autorisation des compartiments empêchent Macie d'accéder aux compartiments et aux objets des compartiments.
- Des compartiments qui ne stockent aucun objet classifiable. Macie ne peut analyser aucun objet dans ces compartiments, car tous les objets utilisent des classes de stockage Amazon S3 non prises en charge par Macie, ou ils ont des extensions de nom de fichier pour des formats de fichier ou de stockage non pris en charge par Macie.
- Des compartiments que Macie n'a pas encore pu analyser en raison d'erreurs de classification au niveau des objets. Macie a tenté d'analyser un ou plusieurs objets contenus dans ces compartiments. Cependant, Macie n'a pas pu analyser les objets en raison de problèmes liés aux paramètres des autorisations au niveau des objets, au contenu des objets ou aux quotas.

Les données de couverture sont mises à jour au fur et à mesure que la découverte automatique des données sensibles progresse chaque jour. Si vous êtes l'administrateur Macie d'une organisation, les données incluent des informations relatives aux compartiments S3 que possèdent vos comptes membres.

> **Note**
>
> Les données de couverture n'incluent pas explicitement les résultats des tâches de découverte de données sensibles que vous avez créées et exécutées. Cependant, la résolution des problèmes de couverture qui affectent vos résultats de découverte automatique de données sensibles est également susceptible d'augmenter la couverture

par les tâches de découverte de données sensibles que vous exécutez ultérieurement. Pour évaluer la couverture d'un emploi, examinez les statistiques et les résultats du poste. Si les événements enregistrés dans le journal d'une tâche ou d'autres résultats indiquent des problèmes de couverture, les conseils de correction présentés plus loin dans cette section peuvent vous aider à résoudre certains de ces problèmes.

Pour examiner les données de couverture relatives à la découverte automatique des données sensibles

Vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie pour consulter les données de couverture de votre compte ou de votre organisation. Sur la console, une seule page fournit une vue unifiée des données de couverture pour tous vos compartiments S3 à usage général, y compris un récapitulatif des problèmes récemment survenus pour chaque compartiment. La page propose également des options permettant de consulter des groupes de données par type de problème. Pour suivre votre enquête sur les problèmes liés à des compartiments spécifiques, vous pouvez exporter les données de la page vers un fichier CSV (valeurs séparées par des virgules).

Console

Suivez ces étapes pour consulter les données de couverture relatives à la découverte automatique de données sensibles à l'aide de la console Amazon Macie.

Pour consulter les données de couverture

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Resource coverage.
3. Sur la page Couverture des ressources, choisissez l'onglet correspondant au type de données de couverture que vous souhaitez consulter :

   - Tout — Répertorie tous les compartiments que Macie surveille et analyse pour votre compte.

     Pour chaque compartiment, le champ Problèmes indique si des problèmes ont empêché Macie d'analyser les objets du compartiment. Si la valeur de ce champ est None, Macie a analysé au moins un des objets du compartiment ou Macie n'a encore tenté d'analyser aucun des objets du compartiment. S'il y a des problèmes, ce champ indique la nature des problèmes et la manière de les résoudre. Pour les erreurs de classification au niveau de l'objet, il peut également indiquer (entre parenthèses) le nombre d'occurrences de l'erreur.

- Accès refusé — Répertorie les compartiments auxquels Macie n'est pas autorisé à accéder. Les paramètres d'autorisation pour ces compartiments empêchent Macie d'accéder aux compartiments et aux objets des compartiments. Par conséquent, Macie ne peut analyser aucun objet dans ces compartiments.
- Erreur de classification : répertorie les compartiments que Macie n'a pas encore analysés en raison d'erreurs de classification au niveau des objets (problèmes liés aux paramètres des autorisations au niveau des objets, au contenu des objets ou aux quotas).

  Pour chaque compartiment, le champ Problèmes indique la nature de chaque type d'erreur qui s'est produit et a empêché Macie d'analyser un objet dans le compartiment. Il indique également comment corriger chaque type d'erreur. En fonction de l'erreur, il peut également indiquer (entre parenthèses) le nombre d'occurrences de l'erreur.
- Inclassable : répertorie les compartiments que Macie ne peut pas analyser car ils ne contiennent aucun objet classable. Tous les objets de ces compartiments utilisent des classes de stockage Amazon S3 non prises en charge ou possèdent des extensions de nom de fichier pour des formats de fichier ou de stockage non pris en charge. Par conséquent, Macie ne peut analyser aucun objet dans ces compartiments.

4. Pour effectuer une analyse détaillée et consulter les données de support d'un bucket, choisissez le nom du bucket. Reportez-vous ensuite au panneau des détails du compartiment pour obtenir des statistiques et d'autres informations sur le compartiment.
5. Pour exporter le tableau vers un fichier CSV, choisissez Exporter au format CSV en haut de la page. Le fichier CSV obtenu contient un sous-ensemble de métadonnées pour chaque compartiment du tableau, pour un maximum de 50 000 compartiments. Le fichier inclut un champ Problèmes de couverture. La valeur de ce champ indique si des problèmes ont empêché Macie d'analyser les objets du compartiment et, dans l'affirmative, la nature des problèmes.

API

Pour examiner les données de couverture par programmation, spécifiez des critères de filtre dans les requêtes que vous soumettez à l'aide DescribeBucketsde l'API Amazon Macie. Cette opération renvoie un tableau d'objets. Chaque objet contient des données statistiques et d'autres informations sur un compartiment S3 à usage général répondant aux critères du filtre.

Dans les critères de filtre, incluez une condition pour le type de données de couverture que vous souhaitez examiner :

- Pour identifier les compartiments auxquels Macie n'est pas autorisé à accéder en raison des paramètres d'autorisation des compartiments, incluez une condition selon laquelle la valeur du champ est égale à. `errorCode` `ACCESS_DENIED`
- Pour identifier les compartiments auxquels Macie est autorisé à accéder et qu'il n'a pas encore analysés, incluez les conditions dans lesquelles la valeur du `sensitivityScore` champ est égale `50` et la valeur du `errorCode` champ n'est pas égale. `ACCESS_DENIED`
- Pour identifier les compartiments que Macie ne peut pas analyser parce que tous leurs objets utilisent des classes ou des formats de stockage non pris en charge, incluez les conditions dans lesquelles la valeur du `classifiableSizeInBytes` champ est égale `0` et la valeur du champ est supérieure à. `sizeInBytes` `0`
- Pour identifier les compartiments pour lesquels Macie a analysé au moins un objet, incluez les conditions dans lesquelles la valeur du `sensitivityScore` champ se situe entre 1 et 99 mais n'est pas égale à. `50` Pour inclure également les compartiments dans lesquels vous avez attribué manuellement le score maximum, la plage doit être comprise entre 1 et 100.
- Pour identifier les compartiments que Macie n'a pas encore analysés en raison d'erreurs de classification au niveau des objets, incluez une condition selon laquelle la valeur du champ est égale à. `sensitivityScore` `-1` Pour ensuite passer en revue le détail des types et du nombre d'erreurs survenues pour un compartiment donné, utilisez l'GetResourceProfileopération.

Si vous utilisez le AWS Command Line Interface (AWS CLI), spécifiez les critères de filtre dans les requêtes que vous soumettez en exécutant la commande describe-buckets. Pour consulter le détail des types et du nombre d'erreurs survenues pour un compartiment S3 donné, le cas échéant, exécutez la get-resource-profilecommande.

Par exemple, les AWS CLI commandes suivantes utilisent des critères de filtre pour récupérer les détails de tous les compartiments S3 auxquels Macie n'est pas autorisé à accéder en raison des paramètres d'autorisation des compartiments.

Cet exemple est formaté pour Linux, macOS ou Unix :

```
$ aws macie2 describe-buckets --criteria '{"errorCode":{"eq":["ACCESS_DENIED"]}}'
```

Cet exemple est formaté pour Microsoft Windows :

```
C:\> aws macie2 describe-buckets --criteria={\"errorCode\":{\"eq\":[\"ACCESS_DENIED
\"]}}
```

Si votre demande aboutit, Macie renvoie un `buckets` tableau. Le tableau contient un objet pour chaque compartiment S3 présent dans le compartiment actuel Région AWS et répondant aux critères du filtre.

Si aucun compartiment S3 ne correspond aux critères du filtre, Macie renvoie un tableau vide. `buckets`

```
{
    "buckets": []
}
```

Pour plus d'informations sur la spécification de critères de filtre dans les requêtes, notamment des exemples de critères courants, consultezFiltrer l'inventaire de votre compartiment S3.

Résolution des problèmes de couverture pour la découverte automatique des données sensibles

Amazon Macie signale plusieurs types de problèmes qui réduisent la couverture de vos données Amazon Simple Storage Service (Amazon S3) par la découverte automatique des données sensibles. Les informations suivantes peuvent vous aider à étudier et à résoudre ces problèmes.

Types de problèmes et détails

- Accès refusé
- Erreur de classification : contenu non valide
- Erreur de classification : chiffrement non valide
- Erreur de classification : clé KMS non valide
- Erreur de classification : autorisation refusée
- Inclassable

> **Tip**
>
> Pour étudier les erreurs de classification au niveau des objets pour un compartiment S3, commencez par consulter la liste des exemples d'objets pour le compartiment. Cette liste

indique les objets que Macie a analysés ou a tenté d'analyser dans le compartiment, pour un maximum de 100 objets.
Pour consulter la liste sur la console Amazon Macie, choisissez le compartiment sur la page des compartiments S3, puis choisissez l'onglet Exemples d'objets dans le panneau des détails du compartiment. Pour consulter la liste par programmation, utilisez l'ListResourceProfileArtifactsAPI Amazon Macie. Si le statut de l'analyse d'un objet est ignoré (`SKIPPED`), l'objet est peut-être à l'origine de l'erreur.

Accès refusé

Ce problème indique que les paramètres d'autorisation d'un compartiment S3 empêchent Macie d'accéder au compartiment et aux objets du compartiment. Macie ne peut récupérer ni analyser aucun objet dans le compartiment.

Détails

La cause la plus courante de ce type de problème est une politique de compartiment restrictive. Une politique de compartiment est une politique basée sur les ressources AWS Identity and Access Management (IAM) qui spécifie les actions qu'un principal (utilisateur, compte, service ou autre entité) peut effectuer sur un compartiment S3, ainsi que les conditions dans lesquelles un principal peut effectuer ces actions. Une politique de compartiment restrictive utilise des `Deny` déclarations explicites `Allow` ou des instructions qui accordent ou limitent l'accès aux données d'un compartiment en fonction de conditions spécifiques. Par exemple, une politique de compartiment peut contenir une `Deny` instruction `Allow` or qui refuse l'accès à un compartiment à moins que des adresses IP source spécifiques ne soient utilisées pour accéder au compartiment.

Si la politique de compartiment d'un compartiment S3 contient une `Deny` déclaration explicite avec une ou plusieurs conditions, Macie ne sera peut-être pas autorisée à récupérer et à analyser les objets du compartiment pour détecter des données sensibles. Macie ne peut fournir qu'un sous-ensemble d'informations sur le bucket, telles que son nom et sa date de création.

Conseils de remédiation

Pour résoudre ce problème, mettez à jour la politique de compartiment pour le compartiment S3. Assurez-vous que la politique autorise Macie à accéder au compartiment et aux objets du compartiment. Pour autoriser cet accès, ajoutez une condition pour le rôle lié au service Macie (`AWSServiceRoleForAmazonMacie`) à la politique. La condition doit empêcher le rôle lié au service Macie de correspondre à la `Deny` restriction de la politique. Il peut le faire en utilisant la

clé de contexte de condition `aws:PrincipalArn` globale et le nom de ressource Amazon (ARN) du rôle lié au service Macie pour votre compte.

Si vous mettez à jour la politique du compartiment et que Macie accède au compartiment S3, Macie détectera le changement. Lorsque cela se produit, Macie met à jour les statistiques, les données d'inventaire et les autres informations qu'il fournit sur vos données Amazon S3. En outre, les objets du compartiment seront analysés en priorité lors d'un cycle d'analyse ultérieur.

Référence supplémentaire

Pour plus d'informations sur la mise à jour d'une politique de compartiment S3 afin de permettre à Macie d'accéder à un compartiment, consultezAutoriser Amazon Macie à accéder aux compartiments et aux objets S3. Pour plus d'informations sur l'utilisation des politiques relatives aux compartiments pour contrôler l'accès aux compartiments, consultez les sections Politiques relatives aux compartiments et politiques utilisateur et Comment Amazon S3 autorise une demande dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Erreur de classification : contenu non valide

Ce type d'erreur de classification se produit si Macie tente d'analyser un objet dans un compartiment S3 et que l'objet est mal formé ou que le contenu de l'objet dépasse le quota de découverte de données sensibles. Macie ne peut pas analyser l'objet.

Détails

Cette erreur se produit généralement parce qu'un objet S3 est un fichier mal formé ou endommagé. Par conséquent, Macie ne peut pas analyser et analyser toutes les données du fichier.

Cette erreur peut également se produire si l'analyse d'un objet S3 dépasse le quota de découverte de données sensibles pour un fichier individuel. Par exemple, la taille de stockage de l'objet dépasse le quota de taille pour ce type de fichier.

Dans les deux cas, Macie ne peut pas terminer son analyse de l'objet S3 et le statut de l'analyse de l'objet est ignoré ()`SKIPPED`.

Conseils de remédiation

Pour examiner cette erreur, téléchargez l'objet S3 et vérifiez le formatage et le contenu du fichier. Évaluez également le contenu du fichier par rapport aux quotas Macie pour la découverte de données sensibles.

Si vous ne corrigez pas cette erreur, Macie essaiera d'analyser les autres objets du compartiment S3. Si Macie analyse un autre objet avec succès, Macie mettra à jour les données de couverture et les autres informations fournies sur le compartiment.

Référence supplémentaire

Pour obtenir la liste des quotas de découverte de données sensibles, y compris les quotas pour certains types de fichiers, consultezQuotas Amazon Macie. Pour plus d'informations sur la façon dont Macie met à jour les scores de sensibilité et les autres informations qu'il fournit sur les compartiments S3, consultez. Comment fonctionne la découverte automatique des données sensibles

Erreur de classification : chiffrement non valide

Ce type d'erreur de classification se produit si Macie tente d'analyser un objet dans un compartiment S3 et que l'objet est chiffré à l'aide d'une clé fournie par le client. L'objet utilise le chiffrement SSE-C, ce qui signifie que Macie ne peut ni récupérer ni analyser l'objet.

Détails

Amazon S3 prend en charge plusieurs options de chiffrement pour les objets S3. Pour la plupart de ces options, Macie peut déchiffrer un objet en utilisant le rôle lié au service Macie pour votre compte. Cela dépend toutefois du type de chiffrement utilisé.

Pour que Macie puisse déchiffrer un objet S3, celui-ci doit être chiffré avec une clé à laquelle Macie peut accéder et qu'il est autorisé à utiliser. Si un objet est chiffré à l'aide d'une clé fournie par le client, Macie ne peut pas fournir le matériel de clé requis pour récupérer l'objet sur Amazon S3. Par conséquent, Macie ne peut pas analyser l'objet et le statut de l'analyse de l'objet est ignoré ()`SKIPPED`.

Conseils de remédiation

Pour corriger cette erreur, chiffrez les objets S3 avec des clés gérées ou AWS Key Management Service (AWS KMS) Amazon S3. Si vous préférez utiliser des AWS KMS clés, il peut s'agir de clés KMS AWS gérées ou de clés KMS gérées par le client que Macie est autorisé à utiliser.

Pour chiffrer des objets S3 existants avec des clés auxquelles Macie peut accéder et utiliser, vous pouvez modifier les paramètres de chiffrement des objets. Pour chiffrer de nouveaux objets avec des clés auxquelles Macie peut accéder et utiliser, modifiez les paramètres de chiffrement par défaut du compartiment S3. Assurez-vous également que la politique du compartiment n'exige pas que les nouveaux objets soient chiffrés à l'aide d'une clé fournie par le client.

Si vous ne corrigez pas cette erreur, Macie essaiera d'analyser les autres objets du compartiment S3. Si Macie analyse un autre objet avec succès, Macie mettra à jour les données de couverture et les autres informations fournies sur le compartiment.

Référence supplémentaire

Pour plus d'informations sur les exigences et les options relatives à l'utilisation de Macie pour analyser des objets S3 chiffrés, consultezAnalyse d'objets Amazon S3 chiffrés avec Amazon Macie. Pour plus d'informations sur les options et les paramètres de chiffrement pour les compartiments S3, consultez les sections Protection des données par chiffrement et Configuration du comportement de chiffrement côté serveur par défaut pour les compartiments S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Erreur de classification : clé KMS non valide

Ce type d'erreur de classification se produit si Macie tente d'analyser un objet dans un compartiment S3 et que l'objet est chiffré avec une clé AWS Key Management Service (AWS KMS) qui n'est plus disponible. Macie ne peut pas récupérer et analyser l'objet.

Détails

AWS KMS fournit des options pour désactiver et supprimer la gestion par AWS KMS keys le client. Si un objet S3 est chiffré avec une clé KMS désactivée, dont la suppression est prévue ou qui a été supprimée, Macie ne peut ni récupérer ni déchiffrer l'objet. Par conséquent, Macie ne peut pas analyser l'objet et le statut de l'analyse de l'objet est ignoré ()`SKIPPED`. Pour que Macie puisse analyser un objet chiffré, celui-ci doit être chiffré avec une clé à laquelle Macie peut accéder et qu'il est autorisé à utiliser.

Conseils de remédiation

Pour corriger cette erreur, réactivez ou annulez la suppression planifiée de la clé applicable AWS KMS key, en fonction de l'état actuel de la clé. Si la clé applicable a déjà été supprimée, cette erreur ne peut pas être corrigée.

Pour déterminer lequel AWS KMS key a été utilisé pour chiffrer un objet S3, vous pouvez commencer par utiliser Macie pour vérifier les paramètres de chiffrement côté serveur du compartiment S3. Si les paramètres de chiffrement par défaut du compartiment sont configurés pour utiliser une clé KMS, les détails du compartiment indiquent quelle clé est utilisée. Vous pouvez ensuite vérifier l'état de cette clé. Vous pouvez également utiliser Amazon S3 pour vérifier les paramètres de chiffrement du compartiment et des objets individuels qu'il contient.

Si vous ne corrigez pas cette erreur, Macie essaiera d'analyser les autres objets du compartiment S3. Si Macie analyse un autre objet avec succès, Macie mettra à jour les données de couverture et les autres informations fournies sur le compartiment.

Référence supplémentaire

Pour plus d'informations sur l'utilisation de Macie pour vérifier les paramètres de chiffrement côté serveur d'un compartiment S3, consultez. Examiner les détails des compartiments S3 Pour plus d'informations sur la réactivation ou l'annulation de la suppression planifiée d'un AWS KMS key, voir Activation et désactivation des clés et Planification et annulation de la suppression de clés dans le guide du développeur.AWS Key Management Service

Erreur de classification : autorisation refusée

Ce type d'erreur de classification se produit si Macie tente d'analyser un objet dans un compartiment S3 et qu'il ne parvient pas à récupérer ou à déchiffrer l'objet en raison des paramètres d'autorisation de l'objet ou des paramètres d'autorisation de la clé utilisée pour chiffrer l'objet. Macie ne peut pas récupérer et analyser l'objet.

Détails

Cette erreur se produit généralement parce qu'un objet S3 est chiffré avec une clé gérée par le client AWS Key Management Service (AWS KMS) que Macie n'est pas autorisée à utiliser. Si un objet est chiffré et géré par un client AWS KMS key, la politique de la clé doit autoriser Macie à déchiffrer les données à l'aide de la clé.

Cette erreur peut également se produire si les paramètres d'autorisation d'Amazon S3 empêchent Macie de récupérer un objet S3. La politique de compartiment pour le compartiment S3 peut restreindre l'accès à des objets de compartiment spécifiques ou autoriser uniquement certains principaux (utilisateurs, comptes, services ou autres entités) à accéder aux objets. La liste de contrôle d'accès (ACL) d'un objet peut également restreindre l'accès à celui-ci. Par conséquent, Macie pourrait ne pas être autorisé à accéder à l'objet.

Dans les cas précédents, Macie ne peut pas récupérer et analyser l'objet, et le statut de l'analyse de l'objet est ignoré ()`SKIPPED`.

Conseils de remédiation

Pour corriger cette erreur, déterminez si l'objet S3 est chiffré avec un compte géré AWS KMS key par le client. Si tel est le cas, assurez-vous que la politique de la clé autorise le rôle lié au service Macie (`AWSServiceRoleForAmazonMacie`) à déchiffrer les données avec la clé. La manière

dont vous autorisez cet accès dépend du fait que le compte propriétaire possède AWS KMS key également le compartiment S3 qui stocke l'objet. Si le même compte possède la clé KMS et le bucket, un utilisateur du compte doit mettre à jour la politique de la clé. Si un compte possède la clé KMS et qu'un autre compte possède le compartiment, un utilisateur du compte propriétaire de la clé doit autoriser l'accès entre comptes à la clé.

> **Tip**
>
> Vous pouvez générer automatiquement une liste de tous les clients gérés AWS KMS keys auxquels Macie doit accéder pour analyser les objets contenus dans les compartiments S3 de votre compte. Pour ce faire, exécutez le script AWS KMS Permission Analyzer, disponible dans le référentiel Amazon Macie Scripts sur. GitHub Le script peut également générer un script supplémentaire de commandes AWS Command Line Interface (AWS CLI). Vous pouvez éventuellement exécuter ces commandes pour mettre à jour les paramètres de configuration et les politiques requis pour les clés KMS que vous spécifiez.

Si Macie est déjà autorisé à utiliser la clé applicable AWS KMS key ou si l'objet S3 n'est pas chiffré avec une clé KMS gérée par le client, assurez-vous que la politique du bucket autorise Macie à accéder à l'objet. Vérifiez également que l'ACL de l'objet autorise Macie à lire les données et les métadonnées de l'objet.

Pour la politique du bucket, vous pouvez autoriser cet accès en ajoutant une condition pour le rôle lié au service Macie à la politique. La condition doit empêcher le rôle lié au service Macie de correspondre à la `Deny` restriction de la politique. Il peut le faire en utilisant la clé de contexte de condition `aws:PrincipalArn` globale et le nom de ressource Amazon (ARN) du rôle lié au service Macie pour votre compte.

Pour l'ACL de l'objet, vous pouvez autoriser cet accès en collaborant avec le propriétaire de l'objet pour vous ajouter Compte AWS en tant que bénéficiaire avec `READ` des autorisations pour l'objet. Macie peut ensuite utiliser le rôle lié au service associé à votre compte pour récupérer et analyser l'objet. Pensez également à modifier les paramètres de propriété de l'objet pour le bucket. Vous pouvez utiliser ces paramètres pour désactiver les ACL pour tous les objets du compartiment et accorder des autorisations de propriété au compte propriétaire du compartiment.

Si vous ne corrigez pas cette erreur, Macie essaiera d'analyser les autres objets du compartiment S3. Si Macie analyse un autre objet avec succès, Macie mettra à jour les données de couverture et les autres informations fournies sur le compartiment.

Référence supplémentaire

Pour plus d'informations sur l'autorisation à Macie de déchiffrer des données gérées par un client AWS KMS key, consultez. Autoriser Amazon Macie à utiliser un service géré par le client AWS KMS key Pour plus d'informations sur la mise à jour d'une politique de compartiment S3 afin de permettre à Macie d'accéder à un compartiment, consultezAutoriser Amazon Macie à accéder aux compartiments et aux objets S3.

Pour plus d'informations sur la mise à jour d'une politique clé, consultez la section Modification d'une politique clé dans le Guide du AWS Key Management Service développeur. Pour plus d'informations sur l'utilisation d'objets S3 gérés par AWS KMS keys le client, consultez la section Utilisation du chiffrement côté serveur avec des AWS KMS clés dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Pour plus d'informations sur l'utilisation des politiques de compartiment pour contrôler l'accès aux compartiments S3, consultez les sections Politiques relatives aux compartiments et politiques utilisateur et Comment Amazon S3 autorise une demande dans le guide de l'utilisateur d'Amazon Simple Storage Service. Pour plus d'informations sur l'utilisation des ACL ou des paramètres de propriété des objets pour contrôler l'accès aux objets S3, consultez la section Gestion de l'accès à l'aide des ACL, contrôle de la propriété des objets et désactivation des ACL pour votre compartiment dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Inclassable

Ce problème indique que tous les objets d'un compartiment S3 sont stockés à l'aide de classes de stockage Amazon S3 non prises en charge ou de formats de fichiers ou de stockage non pris en charge. Macie ne peut analyser aucun objet dans le compartiment.

Détails

Pour être éligible à la sélection et à l'analyse, un objet S3 doit utiliser une classe de stockage Amazon S3 prise en charge par Macie. L'objet doit également avoir une extension de nom de fichier pour un format de fichier ou de stockage pris en charge par Macie. Si un objet ne répond pas à ces critères, il est traité comme un objet inclassable. Macie n'essaie pas de récupérer ou d'analyser des données dans des objets inclassables.

Si tous les objets d'un compartiment S3 sont des objets inclassables, le compartiment global est un compartiment inclassable. Macie ne peut pas effectuer de découverte automatique de données sensibles pour le compartiment.

Conseils de remédiation

Pour résoudre ce problème, passez en revue les règles de configuration du cycle de vie et les autres paramètres qui déterminent les classes de stockage utilisées pour stocker les objets dans le compartiment S3. Envisagez d'ajuster ces paramètres pour utiliser les classes de stockage prises en charge par Macie. Vous pouvez également modifier la classe de stockage des objets existants dans le compartiment.

Évaluez également les formats de fichier et de stockage des objets existants dans le compartiment S3. Pour analyser les objets, envisagez de porter les données, temporairement ou définitivement, vers de nouveaux objets utilisant un format pris en charge.

Si des objets sont ajoutés au compartiment S3 et qu'ils utilisent une classe et un format de stockage pris en charge, Macie détectera les objets lors de la prochaine évaluation de votre inventaire de compartiments. Dans ce cas, Macie cessera de signaler que le compartiment est inclassable en termes de statistiques, de données de couverture et d'autres informations qu'il fournit sur vos données Amazon S3. En outre, les nouveaux objets seront analysés en priorité lors d'un cycle d'analyse ultérieur.

Référence supplémentaire

Pour plus d'informations sur les classes de stockage Amazon S3 et les formats de fichiers et de stockage pris en charge par Macie, consultezClasses et formats de stockage pris en charge par Amazon Macie. Pour plus d'informations sur les règles de configuration du cycle de vie et les options de classe de stockage proposées par Amazon S3, consultez les sections Gestion du cycle de vie du stockage et Utilisation des classes de stockage Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Examen des statistiques et des résultats de découverte automatique de données sensibles

Si la découverte automatique des données sensibles est activée, Amazon Macie génère et gère automatiquement des données d'inventaire, des statistiques et d'autres informations supplémentaires sur les compartiments à usage général Amazon Simple Storage Service (Amazon S3) qu'il surveille et analyse pour votre compte. Si vous êtes l'administrateur Macie d'une organisation, cela inclut par défaut les compartiments S3 que possèdent vos comptes membres.

Les informations supplémentaires capturent les résultats des activités automatisées de découverte de données sensibles effectuées par Macie jusqu'à présent. Elle complète également les autres

informations fournies par Macie concernant vos données Amazon S3, telles que les paramètres d'accès public et de chiffrement pour les compartiments S3 individuels. Outre les métadonnées et les statistiques, Macie produit des enregistrements des données sensibles qu'elle trouve et des analyses qu'elle effectue, c'est-à-dire les découvertes de données sensibles et les résultats de découverte de données sensibles.

Au fur et à mesure que la découverte automatique des données sensibles progresse chaque jour, les fonctionnalités et données suivantes peuvent vous aider à examiner et à évaluer les résultats :

- Tableau de bord récapitulatif : fournit des statistiques agrégées pour votre parc de données Amazon S3. Les statistiques incluent des données relatives à des indicateurs clés tels que le nombre total de compartiments dans lesquels Macie a trouvé des données sensibles et le nombre de ces compartiments accessibles au public. Ils signalent également des problèmes qui affectent la couverture de vos données Amazon S3.
- Carte thermique des compartiments S3 : fournit une représentation visuelle interactive de la sensibilité des données dans l'ensemble de votre parc de données, regroupée par Compte AWS. Pour chaque compte, la carte inclut des statistiques de sensibilité agrégées et utilise des couleurs pour indiquer le score de sensibilité actuel pour chaque compartiment détenu par le compte. La carte utilise également des symboles pour vous aider à identifier les compartiments accessibles au public, qui ne peuvent pas être analysés par Macie, etc.
- Tableau des compartiments S3 : fournit des informations récapitulatives pour chaque compartiment S3 de votre inventaire. Pour chaque compartiment, le tableau inclut des données telles que le score de sensibilité actuel du compartiment, le nombre d'objets que Macie peut analyser dans le compartiment et si vous avez configuré des tâches de découverte de données sensibles pour analyser périodiquement les objets du compartiment. Vous pouvez exporter les données du tableau vers un fichier de valeurs séparées par des virgules (CSV).
- Panneau de détails : fournit des détails et des statistiques pour un compartiment S3 que vous choisissez dans la carte thermique ou le tableau. Les détails incluent une liste des objets que Macie a analysés dans le compartiment, ainsi qu'une ventilation des types et du nombre d'occurrences de données sensibles que Macie a trouvées dans le compartiment. Vous pouvez également utiliser le panneau pour gérer les paramètres de découverte automatique d'un bucket.
- Résultats relatifs aux données sensibles — Fournissez des rapports détaillés sur les données sensibles que Macie trouve dans des objets S3 individuels. Les détails incluent le moment où Macie a trouvé les données sensibles, ainsi que les types et le nombre d'occurrences des données sensibles trouvées par Macie. Les détails incluent également des informations sur le compartiment

et l'objet S3 concernés, notamment les paramètres d'accès public du compartiment et la date de dernière modification de l'objet.

- Résultats de découverte de données sensibles : fournissez des enregistrements de l'analyse effectuée par Macie pour des objets S3 individuels. Cela inclut les objets dans lesquels Macie ne trouve pas de données sensibles et les objets que Macie ne peut pas analyser en raison de problèmes ou d'erreurs. Si Macie trouve des données sensibles dans un objet, le résultat de la découverte des données sensibles fournit des informations sur les données sensibles détectées par Macie.

Grâce à ces données, vous pouvez évaluer la sensibilité des données dans l'ensemble de votre parc de données Amazon S3 et effectuer une analyse approfondie pour évaluer et étudier les compartiments et objets S3 individuels. En combinaison avec les informations fournies par Macie concernant la sécurité et la confidentialité de vos données Amazon S3, vous pouvez également identifier les cas où une correction immédiate peut être nécessaire, par exemple un compartiment accessible au public dans lequel Macie a trouvé des données sensibles.

Des données supplémentaires peuvent vous aider à évaluer et à surveiller la couverture de votre parc de données Amazon S3. Grâce aux données de couverture, vous pouvez vérifier l'état des analyses pour l'ensemble de votre parc de données et pour les compartiments S3 individuels de votre inventaire de compartiments. Vous pouvez également identifier les problèmes qui empêchaient Macie d'analyser des objets dans des compartiments spécifiques. Si vous corrigez les problèmes, vous pouvez augmenter la couverture de vos données Amazon S3 lors des cycles d'analyse suivants. Pour plus d'informations, consultez Évaluation de la couverture de la découverte automatique des données sensibles.

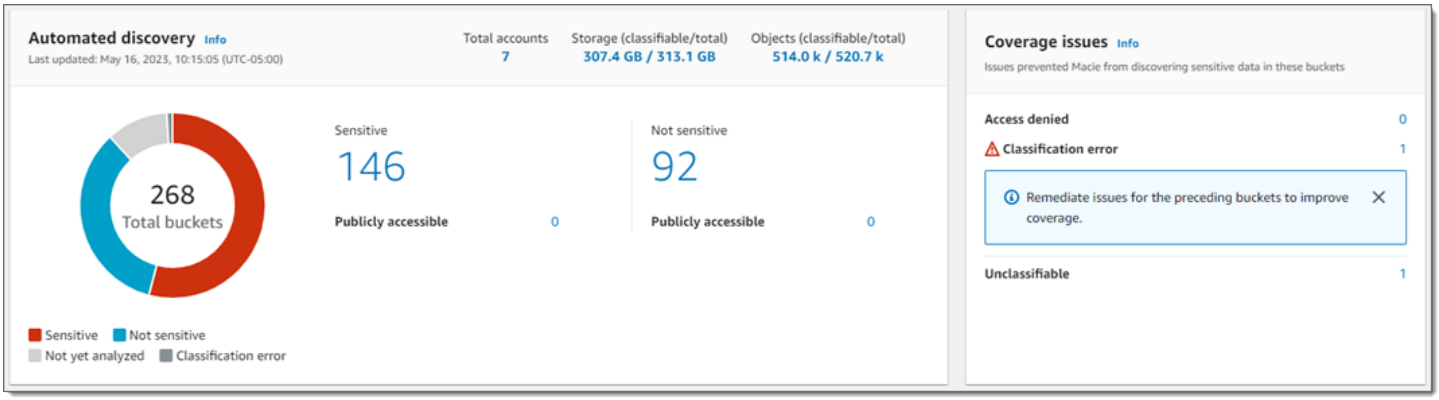
Rubriques

Examen des statistiques agrégées de sensibilité des données sur le tableau de bord récapitulatif

Sur la console Amazon Macie, le tableau de bord récapitulatif fournit un aperçu des statistiques agrégées et des données de résultats pour vos données Amazon Simple Storage Service (Amazon S3) actuelles. Région AWS Il est conçu pour vous aider à évaluer le niveau de sécurité global de vos données Amazon S3.

Les statistiques du tableau de bord incluent des données relatives à des indicateurs de sécurité clés tels que le nombre de compartiments S3 à usage général accessibles au public ou partagés avec d'autres Comptes AWS utilisateurs. Le tableau de bord affiche également des groupes de données de résultats agrégées pour votre compte, par exemple les compartiments qui ont généré le plus de résultats au cours des sept jours précédents. Si vous êtes l'administrateur Macie d'une organisation, le tableau de bord fournit des statistiques et des données agrégées pour tous les comptes de votre organisation. Vous pouvez éventuellement filtrer les données par compte.

Si la découverte automatique des données sensibles est activée, le tableau de bord récapitulatif inclut des statistiques de découverte automatisées. Les statistiques capturent l'état et les résultats des activités automatisées de découverte de données sensibles que Macie a effectuées jusqu'à présent pour vos données Amazon S3. Par exemple :



Les statistiques de la section Découverte automatisée fournissent un aperçu de l'état actuel et des résultats des activités de découverte automatique de données sensibles. Les données n'incluent pas les résultats des tâches de découverte de données sensibles que vous avez créées et exécutées.

Les statistiques de la section Problèmes de couverture indiquent si des problèmes empêchent Macie d'analyser des objets dans des compartiments S3 individuels. Ces statistiques n'incluent pas explicitement les données relatives aux tâches de découverte de données sensibles que vous avez créées et exécutées. Toutefois, la résolution des problèmes de couverture qui affectent vos

résultats de découverte automatique de données sensibles est également susceptible d'augmenter la couverture par les tâches que vous exécuterez par la suite.

Rubriques

Afficher le tableau de bord récapitulatif

Suivez ces étapes pour afficher le tableau de bord récapitulatif sur la console Amazon Macie. Si vous préférez interroger les statistiques par programmation, vous pouvez utiliser le GetBucketStatisticsfonctionnement de l'API Amazon Macie.

Pour afficher le tableau de bord récapitulatif

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Résumé. Macie affiche le tableau de bord récapitulatif.
3. Pour accéder aux données justificatives d'un élément du tableau de bord et passer en revue les données correspondantes, sélectionnez l'élément en question.

Si vous êtes l'administrateur Macie d'une organisation, le tableau de bord affiche des statistiques et des données agrégées pour votre compte et les comptes des membres de votre organisation. Pour filtrer le tableau de bord et afficher les données uniquement pour un compte en particulier, entrez l'identifiant du compte dans le champ Compte situé au-dessus du tableau de bord.

Comprendre les statistiques de découverte automatique de données sensibles sur le tableau de bord récapitulatif

Le tableau de bord récapitulatif de la console Amazon Macie inclut des statistiques agrégées qui peuvent vous aider à surveiller la découverte automatique de données sensibles pour vos données Amazon S3. Il fournit un aperçu de l'état actuel et des résultats des analyses de vos données Amazon S3 actuelles Région AWS.

Par exemple, vous pouvez utiliser les statistiques du tableau de bord pour déterminer rapidement le nombre de compartiments S3 dans lesquels Amazon Macie a détecté des données sensibles, et combien de ces compartiments sont accessibles au public. Vous pouvez également évaluer la

couverture de vos données Amazon S3 et identifier les problèmes qui empêchent Macie d'analyser des objets dans des compartiments S3 individuels.

Sur le tableau de bord, les statistiques de découverte automatique de données sensibles sont principalement organisées dans les sections suivantes :

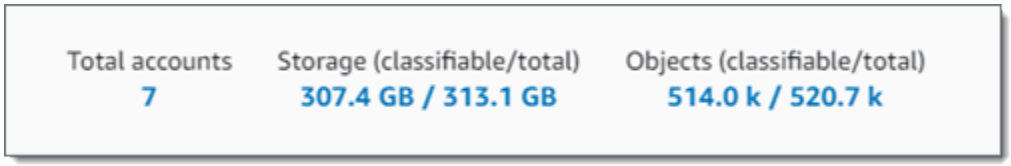
- Stockage et découverte de données sensibles
- Découverte automatisée
- Problèmes de couverture

Lorsque vous passez en revue chaque section, choisissez éventuellement un élément à explorer vers le bas et examinez les données justificatives. Notez également que le tableau de bord n'inclut pas les données relatives aux compartiments de répertoire S3, mais uniquement les compartiments à usage général. Macie ne surveille ni n'analyse les compartiments de répertoires.

Les statistiques individuelles de chaque section sont les suivantes. Pour plus d'informations sur les statistiques dans d'autres sections du tableau de bord récapitulatif, consultezComprendre les composants du tableau de bord récapitulatif.

Stockage et découverte de données sensibles

En haut de la section Découverte automatisée, vous trouverez des statistiques indiquant la quantité de données que vous stockez dans Amazon S3 et la quantité de données que Macie peut analyser pour détecter les données sensibles. Par exemple :



Dans cette section :

- Nombre total de comptes : nombre total de Comptes AWS ces propres compartiments dans votre inventaire de compartiments. Si vous êtes l'administrateur Macie d'une organisation, il s'agit du nombre total de comptes Macie que vous gérez pour votre organisation. Si vous avez un compte Macie autonome, cette valeur est 1.
- Stockage : ces indicateurs fournissent des informations sur la taille de stockage des objets de votre inventaire de compartiments :
  - Classifiable : taille de stockage totale de tous les objets que Macie peut analyser dans les compartiments.

- Total : taille de stockage totale de tous les objets contenus dans les compartiments, y compris les objets que Macie ne peut pas analyser.

Si l'un des objets est un fichier compressé, ces valeurs ne reflètent pas la taille réelle de ces fichiers après leur décompression. Si le versionnement est activé pour l'un des compartiments, ces valeurs sont basées sur la taille de stockage de la dernière version de chaque objet contenu dans ces compartiments.

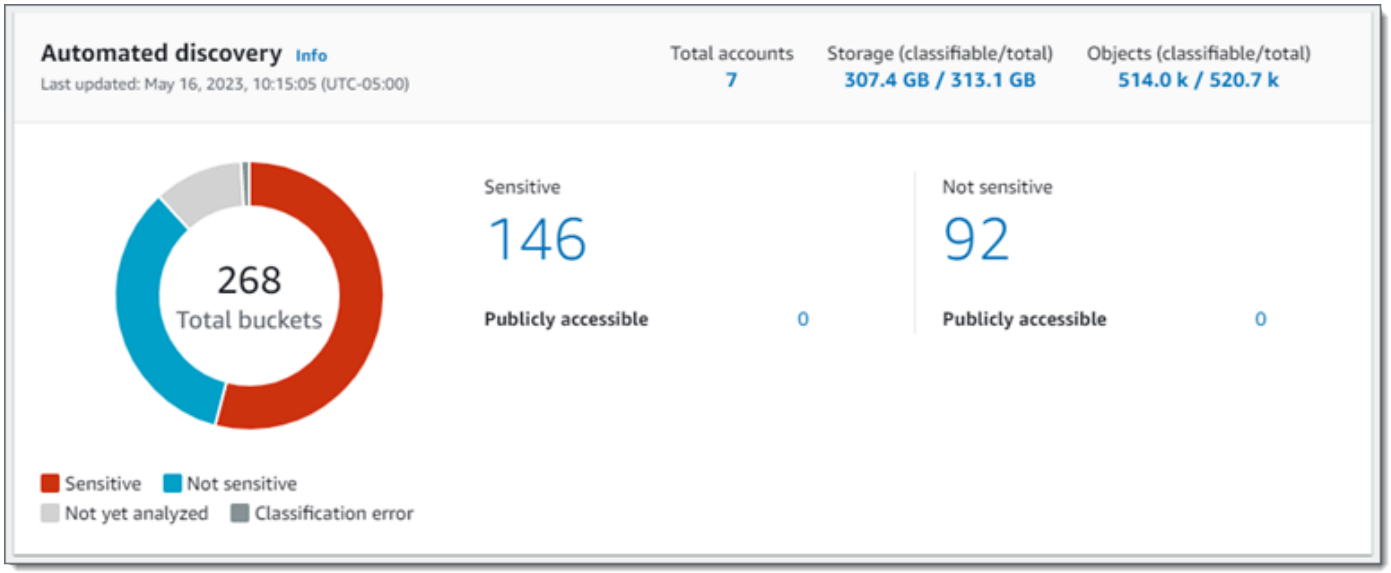
- Objets : ces statistiques fournissent des informations sur le nombre d'objets contenus dans votre inventaire de compartiments :
  - Classifiable : nombre total d'objets que Macie peut analyser dans les compartiments.
  - Total : nombre total d'objets contenus dans les compartiments, y compris les objets que Macie ne peut pas analyser.

Dans les statistiques précédentes, les données et les objets sont classifiables s'ils utilisent une classe de stockage Amazon S3 prise en charge et s'ils possèdent une extension de nom de fichier pour un format de fichier ou de stockage pris en charge. Vous pouvez détecter des données sensibles dans les objets à l'aide de Macie. Pour plus d'informations, consultez Classes et formats de stockage pris en charge.

Notez que les statistiques relatives au stockage et aux objets n'incluent pas les données relatives aux objets contenus dans des compartiments auxquels Macie n'est pas autorisé à accéder. Pour identifier les compartiments dans lesquels c'est le cas, choisissez la statistique Accès refusé dans la section Problèmes de couverture du tableau de bord.

Découverte automatisée

Ces statistiques capturent principalement l'état et les résultats des activités automatisées de découverte de données sensibles que Macie a effectuées jusqu'à présent pour vos données Amazon S3. Par exemple :



Les statistiques individuelles présentées dans cette section sont les suivantes.

Nombre total de seaux

Le tableau en beignets indique le nombre total de seaux dans votre inventaire de seaux. Le graphique regroupe les compartiments en catégories en fonction du score de sensibilité actuel de chaque compartiment :

- Sensible (rouge) : nombre total de compartiments dont le score de sensibilité est compris entre 51 et 100.
- Insensible (bleu) : nombre total de compartiments dont le score de sensibilité est compris entre 1 et 49.
- Pas encore analysé (gris clair) : nombre total de compartiments dont le score de sensibilité est de 50.
- Erreur de classification (gris foncé) : nombre total de compartiments dont le score de sensibilité est de -1.

Pour plus de détails sur la plage de scores de sensibilité et d'étiquettes définie par Macie, voirNotation de sensibilité pour les compartiments S3.

Pour consulter les statistiques supplémentaires d'un groupe, passez le curseur sur le groupe :

- Godets : nombre total de seaux.
- Accessible au public : nombre total de compartiments qui permettent au grand public d'avoir un accès en lecture ou en écriture au compartiment.

- Octets classifiables : taille de stockage totale de tous les objets que Macie peut analyser dans les compartiments. Ces objets utilisent les classes de stockage Amazon S3 prises en charge et possèdent des extensions de nom de fichier pour les formats de fichier ou de stockage pris en charge. Pour plus d'informations, consultez Classes et formats de stockage pris en charge.
- Nombre total d'octets : taille de stockage totale de tous les compartiments.

Dans les statistiques précédentes, les valeurs de taille de stockage sont basées sur la taille de stockage de la dernière version de chaque objet dans les compartiments. Si l'un des objets est un fichier compressé, ces valeurs ne reflètent pas la taille réelle de ces fichiers après leur décompression.

Sensible

Cette zone indique le nombre total de compartiments dont le score de sensibilité est actuellement compris entre 51 et 100. Au sein de ce groupe, Accessible au public indique le nombre total de compartiments qui permettent également au grand public d'avoir un accès en lecture ou en écriture au compartiment.

Non sensible

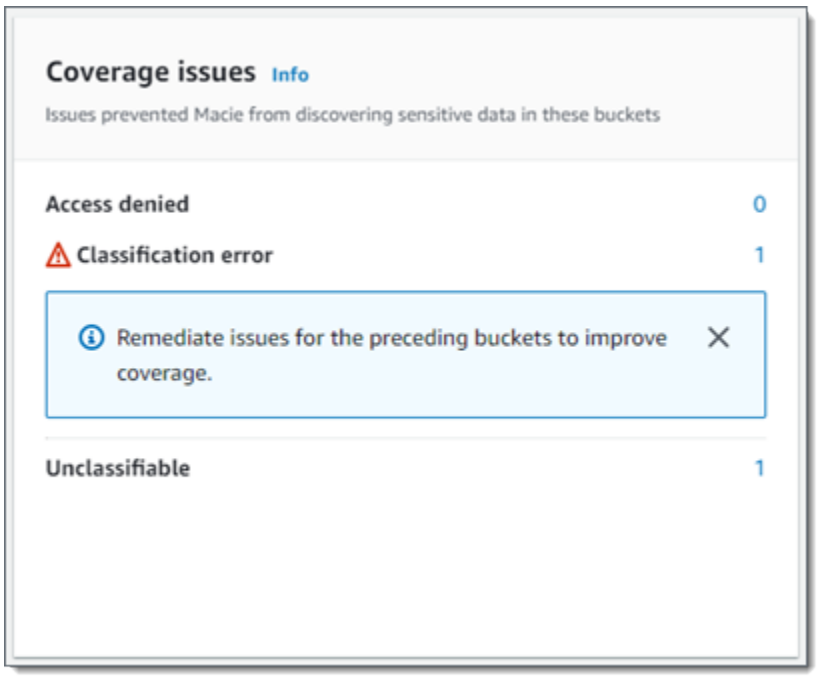
Cette zone indique le nombre total de compartiments dont le score de sensibilité est actuellement compris entre 1 et 49. Au sein de ce groupe, Accessible au public indique le nombre total de compartiments qui permettent également au grand public d'avoir un accès en lecture ou en écriture au compartiment.

Pour déterminer et calculer les valeurs des statistiques accessibles au public, Macie analyse une combinaison de paramètres au niveau du compte et du bucket pour chaque bucket, tels que les paramètres de blocage de l'accès public pour le compte et le bucket, et la politique du bucket pour le bucket. Pour plus d'informations, consultez Comment Macie surveille la sécurité des données Amazon S3.

Notez que les statistiques de la section Découverte automatisée n'incluent pas les résultats des tâches de découverte de données sensibles que vous avez créées et exécutées.

Problèmes de couverture

Ces statistiques indiquent si certains types de problèmes empêchent Macie d'analyser des objets dans des compartiments S3 individuels. Par exemple :



Dans cette section :

- Accès refusé : nombre total de compartiments auxquels Macie n'est pas autorisé à accéder. Macie ne peut analyser aucun objet dans ces compartiments. Les paramètres d'autorisation des compartiments empêchent Macie d'accéder aux compartiments et aux objets des compartiments.
- Erreur de classification : nombre total de compartiments que Macie n'a pas encore analysés en raison d'erreurs de classification au niveau des objets. Macie a essayé d'analyser un ou plusieurs objets contenus dans ces seaux. Cependant, Macie n'a pas pu analyser les objets en raison de problèmes liés aux paramètres des autorisations au niveau des objets, au contenu des objets ou aux quotas.
- Inclassable : nombre total de compartiments qui ne contiennent aucun objet classable. Macie ne peut analyser aucun objet dans ces compartiments. Tous les objets utilisent des classes de stockage Amazon S3 que Macie ne prend pas en charge, ou ils ont des extensions de nom de fichier pour des formats de fichier ou de stockage non pris en charge par Macie.

Choisissez la valeur d'une statistique pour afficher des détails supplémentaires et, le cas échéant, des conseils de correction. Si vous corrigez les problèmes d'accès et les erreurs de classification, vous pouvez augmenter la couverture de vos données Amazon S3 lors des cycles d'analyse suivants. Pour plus d'informations, consultez Évaluation de la couverture de la découverte automatique des données sensibles.

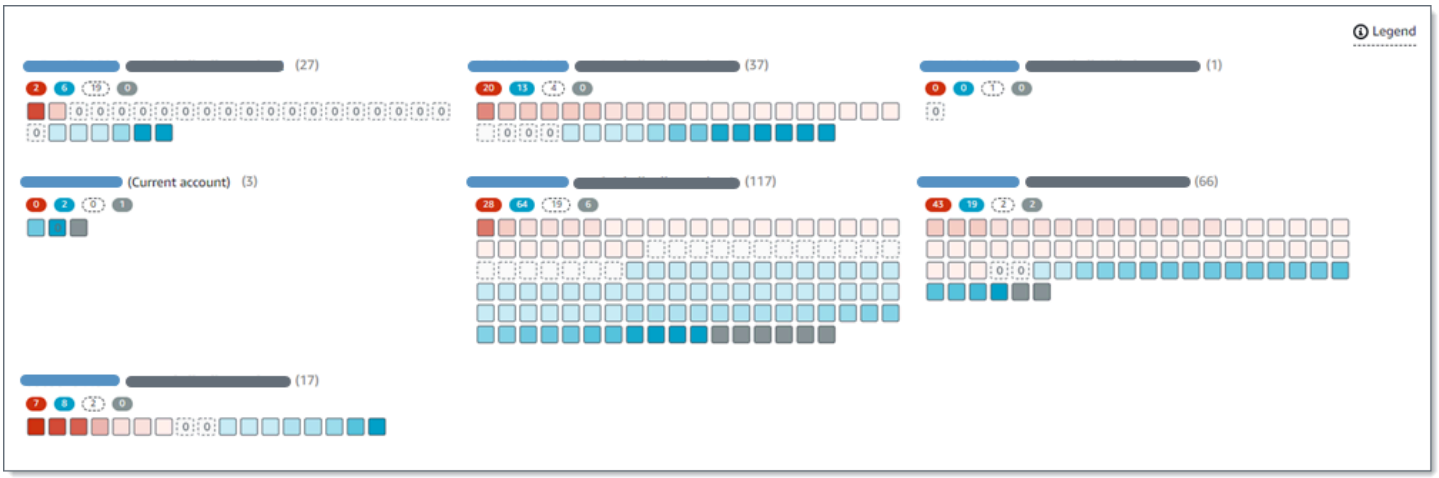
Notez que les statistiques de la section Problèmes de couverture n'incluent pas explicitement les données relatives aux tâches de découverte de données sensibles que vous avez créées et exécutées. Toutefois, la résolution des problèmes de couverture qui affectent vos résultats de découverte automatique de données sensibles est également susceptible d'augmenter la couverture par les tâches que vous exécuterez par la suite.

Pour plus d'informations sur les autres sections du tableau de bord récapitulatif, consultezComprendre les composants du tableau de bord récapitulatif.

Visualisation de la sensibilité des données avec la carte des compartiments S3

Sur la console Amazon Macie, la carte thermique des compartiments S3 fournit une représentation visuelle interactive de la sensibilité des données dans votre parc de données Amazon Simple Storage Service (Amazon S3). Il capture les résultats des activités automatisées de découverte de données sensibles que Macie a effectuées jusqu'à présent pour vos données Amazon S3. Région AWS

Si vous êtes l'administrateur Macie d'une organisation, la carte inclut les résultats pour les compartiments S3 que possèdent vos comptes membres. Les données sont regroupées Compte AWS et triées par numéro de compte. Par exemple :



Chaque page de la carte affiche les données d'un maximum de 99 comptes ou 1 000 compartiments, en fonction de la taille de votre organisation ou du parc de données Amazon S3.

Pour afficher la carte, choisissez les compartiments S3 dans le volet de navigation de la console. Choisissez ensuite map
( )
en haut de la page. La carte n'est disponible que si la découverte automatique des données

sensibles est actuellement activée pour votre compte ou votre organisation. Il n'inclut pas les résultats des tâches de découverte de données sensibles que vous avez créées et exécutées.

Rubriques

- Interprétation des données dans la carte des compartiments S3
- Interaction avec la carte des compartiments S3

Interprétation des données dans la carte des compartiments S3

Dans la carte des compartiments S3, chaque carré représente un compartiment S3 à usage général dans votre inventaire de compartiments. La couleur d'un carré représente le score de sensibilité actuel d'un compartiment, qui mesure l'intersection de deux dimensions principales : la quantité de données sensibles que Macie a trouvées dans le compartiment et la quantité de données que Macie a analysées dans le compartiment. L'intensité de la teinte de la couleur indique où se situe le score d'un bucket dans une plage de valeurs de sensibilité des données, comme le montre l'image suivante.

En général, vous pouvez interpréter l'intensité de la couleur et de la teinte comme suit :

- Bleu — Si le score de sensibilité actuel d'un compartiment est compris entre 1 et 49, le carré du compartiment est bleu et l'étiquette de sensibilité du compartiment est Insensible. L'intensité de la teinte bleue reflète le nombre d'objets uniques analysés par Macie dans le bucket par rapport au nombre total d'objets uniques dans le bucket. Une teinte plus foncée indique un score de sensibilité inférieur.
- Aucune couleur : si le score de sensibilité actuel d'un compartiment est de 50, le carré du compartiment n'est pas coloré et l'étiquette de sensibilité du compartiment n'est pas encore analysée. De plus, le carré possède une bordure en pointillés.
- Rouge — Si le score de sensibilité actuel d'un compartiment est compris entre 51 et 100, le carré du compartiment est rouge et l'étiquette de sensibilité du compartiment est Sensible. L'intensité de la teinte rouge reflète la quantité de données sensibles que Macie a trouvées dans le compartiment. Une teinte plus foncée indique un score de sensibilité plus élevé.

- Gris : si le score de sensibilité actuel d'un compartiment est de -1, le carré du compartiment est gris foncé et l'étiquette de sensibilité du compartiment indique Erreur de classification. L'intensité de la teinte ne varie pas.

Pour plus de détails sur la plage de scores de sensibilité et d'étiquettes définie par Macie, voirNotation de sensibilité pour les compartiments S3.

Sur la carte, le carré d'un compartiment S3 peut également contenir un symbole. Le symbole indique une erreur, un problème ou tout autre type de considération susceptible d'affecter votre évaluation de la sensibilité d'un bucket. Un symbole peut également indiquer un problème potentiel lié à la sécurité du bucket, par exemple, le bucket est accessible au public. Le tableau suivant répertorie les symboles utilisés par Macie pour vous informer de ces cas.

Symbol	Définition	Description
	Accès refusé	Macie n'est pas autorisé à accéder au bucket ou aux objets du bucket. Par conséquent, Macie ne peut analyser aucun objet du compartiment. Ce problème se produit généralement parce qu'un compartiment est soumis à une politique de compartim ent restrictive. Pour plus d'informations sur la manière de résoudre ce problème, consultezAutoriser Macie à accéder aux compartiments et aux objets S3.
	Accessible publiquement	Le grand public dispose d'un accès en lecture ou en écriture au bucket.

Symbol	Définition	Description
		Pour prendre cette décision, Macie analyse une combinaison de paramètres au niveau du compte et du compartiment pour chaque compartiment, tels que les paramètres de blocage de l'accès public pour le compte et le compartiment, et la politique du compartiment pour le compartiment. Pour plus d'informations, consultez Comment Macie surveille la sécurité des données Amazon S3.

Symbol	Définition	Description
	Inclassable	Macie ne peut analyser aucun objet dans le compartiment. Tous les objets du compartiment utilisent des classes de stockage Amazon S3 que Macie ne prend pas en charge, ou ils ont des extensions de nom de fichier pour des formats de fichier ou de stockage non pris en charge par Macie. Pour que Macie puisse analyser un objet, celui-ci doit utiliser une classe de stockage prise en charge et avoir une extension de nom de fichier pour un format de fichier ou de stockage pris en charge. Pour plus d'informations, consultez Classes et formats de stockage pris en charge.
	Zéro octet	Le bucket ne contient aucun objet à analyser par Macie. Le compartiment est vide ou tous les objets qu'il contient ne contiennent aucun (0) octet de données.

Interaction avec la carte des compartiments S3

Lorsque vous consultez la carte des compartiments S3, vous pouvez interagir avec elle de différentes manières pour révéler et évaluer des données et des détails supplémentaires pour des comptes et

des compartiments individuels. Suivez ces étapes pour afficher la carte sur la console Amazon Macie et utiliser les différentes fonctionnalités qu'elle fournit.

Pour interagir avec la carte des compartiments S3

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez S3 buckets (Compartiments S3). La page des compartiments S3 affiche une carte de l'inventaire de vos compartiments. Si la page affiche plutôt votre inventaire sous forme de tableau, choisissez map () en haut de la page.

   Par défaut, la carte n'affiche pas les données relatives aux compartiments actuellement exclus de la découverte automatique de données sensibles. Si vous êtes l'administrateur Macie d'une organisation, elle n'affiche pas non plus les données des comptes pour lesquels la découverte automatique des données sensibles est actuellement désactivée. Pour afficher ces données, choisissez X dans le jeton de filtre Is monitored by automatic discovery situé sous le filtre.
3. En haut de la page, choisissez éventuellement refresh () pour récupérer les dernières métadonnées du bucket depuis Amazon S3.
4. Dans la carte des compartiments S3, effectuez l'une des opérations suivantes :

   - Pour déterminer le nombre de seaux dotés d'une étiquette de sensibilité spécifique, reportez-vous aux badges de couleur situés juste en dessous d'un Compte AWS identifiant. Les badges affichent le nombre de compartiments agrégé, ventilé par étiquette de sensibilité.

     Par exemple, le badge rouge indique le nombre total de buckets détenus par le compte et portant le label Sensitive. Le score de sensibilité de ces seaux est compris entre 51 et 100. Le badge bleu indique le nombre total de compartiments détenus par le compte et portant le label Non sensible. Le score de sensibilité de ces compartiments est compris entre 1 et 49.
   - Pour consulter un sous-ensemble d'informations concernant un compartiment, passez le curseur sur le carré du compartiment. Une fenêtre contextuelle affiche le nom du compartiment et le score de sensibilité actuel.

     La fenêtre contextuelle affiche également le nombre total d'objets que Macie peut analyser dans le compartiment et la taille de stockage totale de la dernière version de ces objets. Ces objets sont classifiables. Ils utilisent les classes de stockage Amazon S3 prises en charge et

possèdent des extensions de nom de fichier pour les formats de fichier ou de stockage pris en charge. Pour plus d'informations, consultez Classes et formats de stockage pris en charge.

- Pour filtrer la carte et n'afficher que les compartiments ayant une valeur spécifique pour un champ, placez votre curseur dans la zone de filtre, puis ajoutez une condition de filtre pour le champ. Macie applique les critères de la condition et affiche la condition sous la boîte de filtre. Pour affiner davantage les résultats, ajoutez des conditions de filtre pour des champs supplémentaires. Pour plus d'informations, consultez Filtrer l'inventaire de votre compartiment S3.
- Pour effectuer une analyse détaillée et afficher uniquement les compartiments appartenant à un compte en particulier, choisissez l'identifiant du compte. Macie ouvre un nouvel onglet qui filtre et affiche les données pour ce compte uniquement.

5. Pour consulter toutes les statistiques de découverte de données sensibles et les autres informations relatives à un compartiment en particulier, choisissez le carré du compartiment, puis reportez-vous au panneau de détails. Pour plus d'informations sur ces détails, consultezExamen des détails relatifs à la sensibilité des données pour les compartiments S3 individuels.

> **Tip**
>
> Dans l'onglet Détails du compartiment du panneau, vous pouvez pivoter et explorer de nombreux champs vers le bas. Pour afficher les compartiments ayant la même valeur pour un champ, choisissez  dans le champ. Pour afficher les compartiments contenant d'autres valeurs pour un champ, choisissez  dans le champ.

Évaluation de la sensibilité des données à l'aide de la table des buckets S3

Sur la console Amazon Macie, le tableau des compartiments S3 affiche des informations récapitulatives sur chacun de vos compartiments à usage général Amazon Simple Storage Service (Amazon S3) actuels. Région AWS Si vous êtes l'administrateur Macie d'une organisation, cela inclut des informations sur les buckets que possèdent vos comptes de membres. Si vous préférez accéder aux données par programmation, vous pouvez utiliser l'DescribeBucketsAPI Amazon Macie.

Sur la console, vous pouvez trier et filtrer le tableau pour personnaliser votre affichage. Vous pouvez également exporter les données du tableau vers un fichier de valeurs séparées par des virgules (CSV). Si vous choisissez un compartiment S3 dans le tableau, le panneau de détails affiche des informations supplémentaires sur le compartiment. Cela inclut des détails et des statistiques sur les paramètres et les mesures qui fournissent un aperçu de la sécurité et de la confidentialité des données du bucket. Si la découverte automatique des données sensibles est activée, elle inclut également les données qui capturent les résultats des activités de découverte automatique que Macie a effectuées pour le bucket jusqu'à présent. Outre l'examen de ces informations, vous pouvez utiliser le panneau pour ajuster les paramètres de découverte automatique d'un bucket. Pour savoir comment procéder, veuillez consulter la section Gestion de la découverte automatisée des données sensibles pour des compartiments S3 individuels.

Pour évaluer la sensibilité des données à l'aide du tableau des compartiments S3

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez S3 buckets (Compartiments S3). La page des compartiments S3 affiche l'inventaire de vos compartiments.

   Par défaut, la page n'affiche pas les données relatives aux compartiments actuellement exclus de la découverte automatique des données sensibles. Si vous êtes l'administrateur Macie d'une organisation, elle n'affiche pas non plus les données des comptes pour lesquels la découverte automatique des données sensibles est actuellement désactivée. Pour afficher ces données, choisissez X dans le jeton de filtre Est surveillé par détection automatique situé sous le filtre.
3. Choisissez table
   ()
   en haut de la page. Macie affiche le nombre de seaux dans votre inventaire et un tableau des seaux.
4. Pour récupérer les dernières métadonnées du bucket depuis Amazon S3, choisissez refresh
   ()
   en haut de la page.

   Si l'icône d'information
   ()
   apparaît à côté d'un nom de bucket, nous vous recommandons de le faire. Cette icône indique qu'un bucket a été créé au cours des dernières 24 heures, probablement après que Macie ait récupéré pour la dernière fois les métadonnées du bucket et de l'objet sur Amazon S3 dans le cadre du cycle d'actualisation quotidien.

5. Dans le tableau des compartiments S3, consultez les informations récapitulatives relatives à chaque compartiment de votre inventaire :

   - Sensibilité : score de sensibilité actuel du compartiment. Pour plus d'informations sur la plage de scores de sensibilité définie par Macie, consultezNotation de sensibilité pour les compartiments S3.
   - Bucket : nom du bucket.
   - Compte : ID de compte du Compte AWS propriétaire du bucket.
   - Objets classifiables : nombre total d'objets que Macie peut analyser pour détecter les données sensibles contenues dans le compartiment.
   - Taille classifiable : taille de stockage totale de tous les objets que Macie peut analyser pour détecter les données sensibles dans le compartiment.

     Cette valeur ne reflète pas la taille réelle des objets compressés après leur décompression. En outre, si le versionnement est activé pour le compartiment, cette valeur est basée sur la taille de stockage de la dernière version de chaque objet du compartiment.
   - Surveillé par tâche : si des tâches de découverte de données sensibles sont configurées pour analyser régulièrement les objets du compartiment sur une base quotidienne, hebdomadaire ou mensuelle.

     Si la valeur de ce champ est Oui, le compartiment est explicitement inclus dans une tâche périodique ou le compartiment a répondu aux critères d'une tâche périodique au cours des dernières 24 heures. En outre, le statut d'au moins un de ces emplois n'est pas annulé. Macie met à jour ces données quotidiennement.
   - Dernière exécution de la tâche : si des tâches ponctuelles ou périodiques de découverte de données sensibles sont configurées pour analyser les objets du compartiment, ce champ indique la date et l'heure les plus récentes auxquelles l'une de ces tâches a commencé à s'exécuter. Dans le cas contraire, un tiret (—) apparaît dans ce champ.

   Dans les données précédentes, les objets sont classifiables s'ils utilisent une classe de stockage Amazon S3 prise en charge et s'ils possèdent une extension de nom de fichier pour un format de fichier ou de stockage pris en charge. Vous pouvez détecter des données sensibles dans les objets à l'aide de Macie. Pour plus d'informations, consultez Classes et formats de stockage pris en charge.
6. Pour analyser votre inventaire à l'aide du tableau, effectuez l'une des opérations suivantes :

- Pour trier le tableau en fonction d'un champ spécifique, choisissez l'en-tête de colonne du champ. Pour modifier l'ordre de tri, choisissez à nouveau l'en-tête de colonne.
- Pour filtrer le tableau et n'afficher que les compartiments contenant une valeur spécifique pour un champ, placez votre curseur dans la zone de filtre, puis ajoutez une condition de filtre pour le champ. Macie applique les critères de la condition et affiche la condition sous la boîte de filtre. Pour affiner davantage les résultats, ajoutez des conditions de filtre pour des champs supplémentaires. Pour plus d'informations, consultez Filtrer l'inventaire de votre compartiment S3.
- Pour consulter les statistiques de découverte de données sensibles et d'autres informations relatives à un bucket en particulier, choisissez le nom du bucket dans le tableau, puis reportez-vous au panneau de détails. Pour plus d'informations sur ces détails, consultezConsulter les détails du bucket S3.

> **Tip**
>
> Dans l'onglet Détails du compartiment du panneau, vous pouvez pivoter et explorer de nombreux champs vers le bas. Pour afficher les compartiments ayant la même valeur pour un champ, choisissez  dans le champ. Pour afficher les compartiments contenant d'autres valeurs pour un champ, choisissez  dans le champ.

7. Pour exporter les données du tableau vers un fichier CSV, cochez la case correspondant à chaque ligne que vous souhaitez exporter ou cochez la case dans l'en-tête de la colonne de sélection pour sélectionner toutes les lignes. Choisissez ensuite Exporter au format CSV en haut de la page. Vous pouvez exporter jusqu'à 50 000 lignes depuis le tableau.
8. Pour effectuer une analyse plus approfondie et plus immédiate des objets contenus dans un ou plusieurs compartiments, cochez la case correspondant à chaque compartiment, puis choisissez Create job. Pour plus d'informations, consultez Création d'une tâche de découverte de données sensibles.

Examen des détails relatifs à la sensibilité des données pour les compartiments S3 individuels

Sur la console Amazon Macie, vous pouvez utiliser le panneau de détails de la page des compartiments S3 pour consulter les statistiques et autres informations relatives à chaque compartiment à usage général Amazon Simple Storage Service (Amazon S3) que Macie surveille et analyse pour votre compte. Si vous êtes l'administrateur Macie d'une organisation, cela inclut les compartiments que possèdent vos comptes membres.

Les statistiques et informations incluent des détails qui donnent un aperçu de la sécurité et de la confidentialité des données d'un compartiment S3. Si la découverte automatique des données sensibles est activée, ils capturent également les résultats des activités de découverte automatique que Macie a effectuées pour un bucket jusqu'à présent. Par exemple, vous pouvez trouver une liste des objets analysés par Macie dans un compartiment, ainsi qu'une ventilation des types et du nombre d'occurrences de données sensibles que Macie a trouvées dans un compartiment. Notez que les données n'incluent pas les résultats des tâches de découverte de données sensibles que vous avez créées et exécutées.

Macie recalcule et met à jour automatiquement ces statistiques et détails pendant qu'il effectue la découverte automatique des données sensibles. Par exemple :

- Si Macie ne trouve aucune donnée sensible dans un objet S3, Macie diminue le score de sensibilité du compartiment et met à jour l'étiquette de sensibilité du compartiment si nécessaire. Macie ajoute également l'objet à la liste des objets analysés dans le compartiment.
- Si Macie trouve des données sensibles dans un objet S3, Macie ajoute ces occurrences à la répartition des types de données sensibles qu'il a trouvés dans le compartiment. Macie augmente également le score de sensibilité du seau et met à jour l'étiquette de sensibilité du seau si nécessaire. En outre, Macie ajoute l'objet à la liste des objets analysés dans le compartiment. Ces tâches s'ajoutent à la création d'une recherche de données sensibles pour l'objet.
- Si Macie trouve des données sensibles dans un objet S3 qui sont ensuite modifiées ou supprimées, Macie supprime les occurrences de données sensibles relatives à cet objet de la ventilation des types de données sensibles du compartiment. Macie diminue également le score de sensibilité du bucket et met à jour l'étiquette de sensibilité du bucket si nécessaire. En outre, Macie supprime l'objet de la liste des objets analysés dans le compartiment.
- Si Macie tente d'analyser un objet S3 mais qu'un problème ou une erreur l'en empêche, Macie ajoute l'objet à la liste des objets analysés dans le compartiment et indique qu'il n'a pas été en mesure d'analyser l'objet.

Outre l'examen des statistiques et des détails, vous pouvez utiliser le panneau pour ajuster les paramètres de découverte automatique des données sensibles pour un compartiment S3. Par exemple, vous pouvez inclure ou exclure des types spécifiques de données sensibles du score d'un bucket. Pour plus d'informations, consultez Gestion de la découverte automatique pour des compartiments S3 individuels.

Pour consulter les informations relatives à la sensibilité des données d'un compartiment S3

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez S3 buckets (Compartiments S3). La page des compartiments S3 affiche une carte interactive de votre inventaire de compartiments. Choisissez éventuellement table () en haut de la page pour afficher votre inventaire sous forme de tableau à la place.

   Par défaut, la page n'affiche pas les données relatives aux compartiments actuellement exclus de la découverte automatique des données sensibles. Si vous êtes l'administrateur Macie d'une organisation, elle n'affiche pas non plus les données des comptes pour lesquels la découverte automatique des données sensibles est actuellement désactivée. Pour afficher ces données, choisissez X dans le jeton de filtre Est surveillé par détection automatique situé sous le filtre.
3. Dans la carte ou le tableau des compartiments S3, choisissez le compartiment S3 dont vous souhaitez consulter les détails. Le panneau de détails affiche des statistiques et d'autres informations sur le bucket.

La partie supérieure du panneau affiche des informations générales sur le bucket : le nom du bucket et l'ID de compte du Compte AWS propriétaire du bucket. Il fournit également des options permettant de modifier certains paramètres de découverte automatique des données sensibles pour le compartiment. Les paramètres et informations supplémentaires concernant le bucket sont organisés dans les onglets suivants :

- Sensibilité
- Détails du godet
- Exemples d'objets
- Découverte de données sensibles

Les paramètres individuels et les informations de chaque onglet sont les suivants.

Sensibilité

Cet onglet indique le score de sensibilité actuel du bucket, compris entre -1 et 100. Pour plus d'informations sur la plage de scores de sensibilité définie par Macie, consultezNotation de sensibilité pour les compartiments S3.

L'onglet fournit également une ventilation des types de données sensibles que Macie a trouvés dans les objets du compartiment, ainsi que le nombre d'occurrences de chaque type :

- Type de données sensibles : identifiant unique (ID) de l'identifiant des données gérées qui a détecté les données, ou nom de l'identifiant de données personnalisé qui a détecté les données.

  L'identifiant d'un identifiant de données géré décrit le type de données sensibles que l'identifiant est conçu pour détecter, par exemple, USA_PASSPORT_NUMBER pour les numéros de passeport américains. Pour plus de détails sur chaque identifiant de données gérées, consultezUtilisation des identificateurs de données gérés.
- Nombre : nombre total d'occurrences des données détectées par l'identifiant de données géré ou personnalisé.
- État de la notation — Spécifie si les occurrences des données sont incluses ou exclues du score de sensibilité du compartiment.

  Si vous avez configuré Macie pour calculer automatiquement le score du bucket, vous pouvez ajuster le calcul en incluant ou en excluant des types spécifiques de données sensibles du score du bucket : cochez la case correspondant à l'identifiant de données que vous souhaitez inclure ou exclure, puis choisissez l'option de votre choix dans le menu Actions. Pour plus d'informations, consultez Gestion de la découverte automatique pour des compartiments S3 individuels.

Si Macie n'a pas trouvé de données sensibles dans les objets que le bucket stocke actuellement, cette section affiche le message Aucune détection trouvée.

Notez que l'onglet Sensibilité n'inclut pas les données relatives aux objets analysés par Macie et qui ont ensuite été modifiés ou supprimés. Si des objets sont modifiés ou supprimés d'un bucket après leur analyse par Macie, Macie recalcule et met à jour automatiquement les statistiques et les données appropriées pour exclure les objets.

Détails du godet

Cet onglet fournit des détails sur les paramètres du bucket, notamment les paramètres de sécurité et de confidentialité des données. Par exemple, vous pouvez consulter le détail des paramètres

d'accès public du compartiment et déterminer si le compartiment réplique des objets ou s'il est partagé avec d'autres. Comptes AWS

Il convient de noter que le champ Dernière mise à jour indique la date à laquelle Macie a récemment récupéré les métadonnées du bucket ou des objets du bucket sur Amazon S3. Le champ Dernière exécution de découverte automatique indique à quel moment Macie a analysé les objets du bucket pour la dernière fois lors de la découverte automatique. Si cette analyse n'a pas eu lieu, un tiret (—) apparaît dans ce champ.

L'onglet fournit également des statistiques au niveau de l'objet qui peuvent vous aider à évaluer la quantité de données que Macie peut analyser dans le compartiment. Il indique également si des tâches de découverte de données sensibles sont configurées pour analyser les objets du compartiment. Si tel est le cas, vous pouvez accéder aux détails de la tâche exécutée le plus récemment, puis éventuellement afficher les résultats produits par la tâche.

Pour plus de détails sur les informations de cet onglet, consultezExaminer les détails des compartiments S3.

Exemples d'objets

Cet onglet répertorie les objets que Macie a sélectionnés pour analyse lors de la découverte automatique des données sensibles pour le compartiment. Choisissez éventuellement le nom d'un objet pour ouvrir la console Amazon S3 et afficher les propriétés de l'objet.

La liste inclut des données pour un maximum de 100 objets. La liste est remplie en fonction de la valeur du champ Sensibilité de l'objet : sensible, suivi de Non sensible, suivi des objets que Macie n'a pas pu analyser.

Dans la liste, le champ Sensibilité de l'objet indique si Macie a trouvé des données sensibles dans un objet :

- Sensible : Macie a détecté au moins une occurrence de données sensibles dans l'objet.
- Non sensible : Macie n'a pas trouvé de données sensibles dans l'objet.
- — (tiret) — Macie n'a pas pu terminer son analyse de l'objet en raison d'un problème ou d'une erreur.

Le champ Résultat de la classification indique si Macie a pu analyser un objet :

- Terminé — Macie a terminé son analyse de l'objet.
- Partiel : Macie n'a analysé qu'un sous-ensemble de données de l'objet en raison d'un problème ou d'une erreur. Par exemple, l'objet est un fichier d'archive contenant des fichiers dans un format non pris en charge.

- Ignoré — Macie n'a pas pu analyser les données de l'objet en raison d'un problème ou d'une erreur. Par exemple, l'objet est chiffré avec une clé que Macie n'est pas autorisée à utiliser.

Notez que la liste n'inclut pas les objets qui ont été modifiés ou supprimés après que Macie les ait analysés ou tenté de les analyser. Macie supprime automatiquement un objet de la liste s'il est modifié ou supprimé ultérieurement.

Découverte de données sensibles

Cet onglet fournit des statistiques agrégées et automatisées de découverte de données sensibles pour le bucket :

- Octets analysés : quantité totale de données, en octets, que Macie a analysées dans le compartiment.
- Octets classifiables : taille de stockage totale, en octets, de tous les objets que Macie peut analyser dans le compartiment. Ces objets utilisent les classes de stockage Amazon S3 prises en charge et possèdent des extensions de nom de fichier pour les formats de fichier ou de stockage pris en charge. Pour plus d'informations, consultez Classes et formats de stockage pris en charge.
- Nombre total de détections : nombre total d'occurrences de données sensibles détectées par Macie dans le compartiment. Cela inclut les occurrences actuellement supprimées par les paramètres de notation de sensibilité du bucket.

Le graphique Objets analysés indique le nombre total d'objets analysés par Macie dans le compartiment. Il fournit également une représentation visuelle du nombre d'objets dans lesquels Macie a trouvé ou n'a pas trouvé de données sensibles. La légende située sous le graphique montre la répartition de ces résultats :

- Objets sensibles (rouge) : nombre total d'objets dans lesquels Macie a détecté au moins une occurrence de données sensibles.
- Objets non sensibles (bleu) : nombre total d'objets dans lesquels Macie n'a pas trouvé de données sensibles.
- Objets ignorés (gris foncé) : nombre total d'objets que Macie n'a pas pu analyser en raison d'un problème ou d'une erreur.

La zone située sous la légende du graphique fournit une ventilation des cas dans lesquels Macie n'a pas pu analyser les objets en raison de certains types de problèmes d'autorisation ou d'erreurs cryptographiques :

- Ignoré : chiffrement non valide — Nombre total d'objets chiffrés à l'aide des clés fournies par le client. Macie ne peut pas accéder à ces clés.

- Ignoré : KMS non valide — Nombre total d'objets chiffrés avec des clés AWS Key Management Service (AWS KMS) qui ne sont plus disponibles. Ces objets sont chiffrés avec ceux AWS KMS keys qui ont été désactivés, dont la suppression est prévue ou qui ont été supprimés. Macie ne peut pas utiliser ces clés.
- Ignoré : autorisation refusée : nombre total d'objets auxquels Macie n'est pas autorisé à accéder en raison des paramètres d'autorisation de l'objet ou des paramètres d'autorisation de la clé utilisée pour chiffrer l'objet.

Pour en savoir plus sur ces problèmes et sur d'autres types de problèmes et d'erreurs susceptibles de se produire, consultezRésolution des problèmes de couverture pour la découverte automatique des données sensibles. Si vous corrigez les problèmes et les erreurs, vous pouvez augmenter la couverture des données du bucket lors des cycles d'analyse suivants.

Les statistiques de l'onglet Découverte des données sensibles n'incluent pas les données relatives aux objets qui ont été modifiés ou supprimés après que Macie les ait analysés ou tenté de les analyser. Si des objets sont modifiés ou supprimés d'un bucket après que Macie les ait analysés ou tenté de les analyser, Macie recalcule automatiquement ces statistiques pour exclure les objets.

Analyse des résultats de données sensibles produits par la découverte automatique

Tout en effectuant la découverte automatique des données sensibles, Amazon Macie crée une recherche de données sensibles pour chaque objet Amazon Simple Storage Service (Amazon S3) dans lequel il trouve des données sensibles. Une découverte de données sensibles est un rapport détaillé des données sensibles que Macie a trouvées dans un objet S3. Chaque découverte de données sensibles fournit une note de gravité et des détails tels que :

- Date et heure auxquelles Macie a trouvé les données sensibles.
- Catégorie et types de données sensibles détectées par Macie.
- Le nombre d'occurrences de chaque type de données sensibles détectées par Macie.
- Comment Macie a trouvé les données sensibles, découverte automatisée des données sensibles ou tâche de découverte de données sensibles.
- Le nom, les paramètres d'accès public, le type de chiffrement et les autres informations relatives au compartiment et à l'objet S3 concernés.

Selon le type de fichier ou le format de stockage de l'objet S3 concerné, les détails peuvent également inclure l'emplacement de 15 occurrences des données sensibles détectées par Macie. Une découverte de données sensibles n'inclut pas les données sensibles trouvées par Macie. Il fournit plutôt des informations que vous pouvez utiliser pour des recherches plus approfondies et des mesures correctives si nécessaire.

Macie conserve les résultats de vos données sensibles pendant 90 jours. Vous pouvez y accéder à l'aide de la console Amazon Macie ou de l'API Amazon Macie. Vous pouvez également surveiller et traiter les résultats à l'aide d'autres applications, services et systèmes. Pour plus d'informations, consultez Analyse des résultats.

Analyser les résultats produits par la découverte automatique de données sensibles

Pour identifier et analyser les résultats créés par Macie lors de la découverte automatique de données sensibles, vous pouvez filtrer vos résultats. Les filtres vous permettent d'utiliser des attributs spécifiques des résultats pour créer des vues personnalisées et des requêtes pour les résultats. Vous pouvez utiliser la console Amazon Macie pour filtrer les résultats ou envoyer des requêtes par programmation à l'aide de l'API Amazon Macie.

Console

Suivez ces étapes pour identifier et analyser les résultats à l'aide de la console Amazon Macie.

Analyser les résultats produits par la découverte automatique

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Conclusions.
3. (Facultatif) Pour afficher les résultats supprimés par une règle de suppression, modifiez le paramètre État des résultats. Choisissez Tout pour afficher à la fois les résultats supprimés et non supprimés, ou choisissez Archivé pour afficher uniquement les résultats supprimés. Pour masquer à nouveau les résultats supprimés, choisissez Current.
4. Placez votre curseur dans la zone Critères de filtre. Dans la liste des champs qui s'affiche, choisissez le type d'origine.

   Ce champ indique comment Macie a trouvé les données sensibles à l'origine d'une découverte, d'une découverte automatisée de données sensibles ou d'une tâche de découverte de données sensibles. Pour trouver ce champ dans la liste des champs de filtre, vous pouvez parcourir la liste complète ou saisir une partie du nom du champ pour affiner la liste des champs.

5. Sélectionnez AUTOMATED_SENSITIVE_DATA_DISCOVERY comme valeur du champ, puis choisissez Appliquer. Macie applique les critères de filtre et ajoute la condition à un jeton de filtre dans la zone Critères de filtre.
6. (Facultatif) Pour affiner les résultats, ajoutez des conditions de filtre pour des champs supplémentaires, par exemple, Created at pour la période pendant laquelle une découverte a été créée, le nom du bucket S3 pour le nom d'un bucket concerné ou le type de détection de données sensibles pour le type de données sensibles qui a été détecté et a produit une constatation. Pour plus d'informations, consultez Filtrage des résultats.

Si vous souhaitez réutiliser cet ensemble de conditions par la suite, vous pouvez l'enregistrer en tant que règle de filtre. Pour ce faire, choisissez Enregistrer la règle dans la zone Critères de filtrage. Entrez ensuite un nom et, éventuellement, une description pour la règle. Lorsque vous avez terminé, choisissez Enregistrer.

API

Pour identifier et analyser les résultats par programmation, spécifiez des critères de filtrage dans les requêtes que vous soumettez à l'aide de l'API Amazon Macie ListFindingsGetFindingStatisticsou à l'aide de celle-ci. L'ListFindingsopération renvoie un tableau d'identifiants de recherche, un identifiant pour chaque résultat correspondant aux critères du filtre. Vous pouvez ensuite utiliser ces identifiants pour récupérer les détails de chaque résultat. L'GetFindingStatisticsopération renvoie des données statistiques agrégées concernant tous les résultats correspondant aux critères du filtre, regroupés selon un champ que vous spécifiez dans votre demande. Pour plus d'informations sur le filtrage des résultats par programmation, consultez. Filtrage des résultats

Dans les critères de filtre, incluez une condition pour le `originType` champ. Ce champ indique comment Macie a trouvé les données sensibles à l'origine d'une découverte, d'une découverte automatisée de données sensibles ou d'une tâche de découverte de données sensibles. La valeur de ce champ indique `AUTOMATED_SENSITIVE_DATA_DISCOVERY` si un résultat a été produit lors d'une découverte automatique.

Pour identifier et analyser les résultats à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande list-findings. get-finding-statistics Les exemples suivants utilisent la list-findings commande pour récupérer les identifiants de recherche pour tous les résultats très graves produits par la découverte automatique de données sensibles dans le présent Région AWS document.

Pour Linux, macOS ou Unix, utilisez la barre oblique inverse (\) pour améliorer la lisibilité :

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"classificationDetails.originType":{"eq":
["AUTOMATED_SENSITIVE_DATA_DISCOVERY"]},"severity.description":{"eq":["High"]}}}'
```

Pour Microsoft Windows, utilisez le caractère de continuation de ligne caret (^) pour améliorer la lisibilité :

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":{\"classificationDetails.originType\":{\"eq
\":[\"AUTOMATED_SENSITIVE_DATA_DISCOVERY\"]},\"severity.description\":{\"eq\":
[\"High\"]}}}
```

Où :

- `classificationDetails.originType`spécifie le nom JSON du champ de type d'origine, et :
  - `eq`spécifie l'opérateur égal.
  - `AUTOMATED_SENSITIVE_DATA_DISCOVERY`est une valeur énumérée pour le champ.
- *`severity.description`*spécifie le nom JSON du champ Severity, et :
  - *`eq`*spécifie l'opérateur égal.
  - *`High`*est une valeur énumérée pour le champ.

Si la commande s'exécute correctement, Macie renvoie un `findingIds` tableau. Le tableau répertorie l'identifiant unique pour chaque résultat correspondant aux critères du filtre, comme illustré dans l'exemple suivant.

```
{
    "findingIds": [
        "1f1c2d74db5d8caa76859ec52example",
        "6cfa9ac820dd6d55cad30d851example",
        "702a6fd8750e567d1a3a63138example",
        "826e94e2a820312f9f964cf60example",
        "274511c3fdcd87010a19a3a42example"
    ]
}
```

Si aucun résultat ne correspond aux critères du filtre, Macie renvoie un `findingIds` tableau vide.

```
{
    "findingIds": []
}
```

Accès aux résultats de découverte de données sensibles produits par la découverte automatique

Amazon Macie crée un enregistrement d'analyse pour chaque objet Amazon Simple Storage Service (Amazon S3) sélectionné pour analyse pendant qu'il effectue la découverte automatique de données sensibles. Ces enregistrements, appelés résultats de découverte de données sensibles, enregistrent les détails de l'analyse que Macie effectue sur des objets S3 individuels. Cela inclut les objets dans lesquels Macie ne trouve pas de données sensibles et les objets que Macie ne peut pas analyser en raison d'erreurs ou de problèmes tels que les paramètres d'autorisation ou l'utilisation d'un format de fichier ou de stockage non pris en charge.

Si Macie trouve des données sensibles dans un objet S3, le résultat de la découverte des données sensibles fournit des informations sur les données sensibles détectées par Macie. Les informations incluent les mêmes types de détails que ceux fournis par une découverte de données sensibles. Il fournit également des informations supplémentaires, telles que l'emplacement de pas moins de 1 000 occurrences de chaque type de données sensibles détectées par Macie. Par exemple :

- Numéro de colonne et de ligne d'une cellule ou d'un champ dans un classeur Microsoft Excel, un fichier CSV ou un fichier TSV
- Le chemin d'accès à un champ ou à un tableau dans un fichier JSON ou JSON Lines
- Numéro de ligne d'une ligne dans un fichier texte non binaire autre qu'un fichier CSV, JSON, JSON Lines ou TSV, par exemple un fichier HTML, TXT ou XML
- Numéro de page d'une page dans un fichier Adobe Portable Document Format (PDF)
- L'index d'enregistrement et le chemin d'accès à un champ dans un enregistrement d'un conteneur d'objets Apache Avro ou d'un fichier Apache Parquet

Si l'objet S3 concerné est un fichier d'archive, tel qu'un fichier .tar ou .zip, le résultat de la découverte de données sensibles fournit également des données de localisation détaillées pour les occurrences de données sensibles dans des fichiers individuels que Macie a extraits de l'archive. Macie n'inclut pas ces informations dans les résultats de données sensibles pour les fichiers d'archive. Pour signaler les données de localisation, les résultats de découverte de données sensibles utilisent un schéma JSON standardisé.

Un résultat de découverte de données sensibles n'inclut pas les données sensibles trouvées par Macie. Il vous fournit plutôt un enregistrement d'analyse qui peut être utile pour les audits ou enquêtes sur la confidentialité et la protection des données.

Macie conserve les résultats de la découverte de vos données sensibles pendant 90 jours. Vous ne pouvez pas y accéder directement depuis la console Amazon Macie ou via l'API Amazon Macie. Au lieu de cela, vous configurez Macie pour les chiffrer et les stocker dans un compartiment S3. Le bucket peut servir de référentiel définitif à long terme pour tous vos résultats de découverte de données sensibles. Vous pouvez ensuite éventuellement accéder aux résultats de ce référentiel et les interroger.

Pour déterminer où se trouve ce référentiel pour votre compte, choisissez Discovery results dans le volet de navigation de la console Amazon Macie. Pour ce faire par programmation, utilisez le GetClassificationExportConfigurationfonctionnement de l'API Amazon Macie. Si vous n'avez pas configuré ce référentiel pour votre compte, consultez la section Stockage et conservation des résultats de découverte de données sensibles pour savoir comment procéder.

Après avoir configuré Macie pour stocker les résultats de la découverte de données sensibles dans un compartiment S3, Macie écrit les résultats dans des fichiers JSON Lines (.jsonl), puis chiffre et ajoute ces fichiers au compartiment sous forme de fichiers GNU Zip (.gz). Pour la découverte automatique des données sensibles, Macie ajoute les fichiers dans un dossier nommé `automated-sensitive-data-discovery` dans le compartiment.

Comme c'est le cas pour les découvertes de données sensibles, les résultats de découverte de données sensibles respectent un schéma standardisé. Cela peut éventuellement vous aider à les interroger, à les surveiller et à les traiter à l'aide d'autres applications, services et systèmes.

> **Tip**
>
> Pour un exemple détaillé et instructif de la manière dont vous pouvez interroger et utiliser les résultats de découverte de données sensibles pour analyser et signaler les risques potentiels liés à la sécurité des données, consultez le billet de blog Comment interroger et visualiser les résultats de découverte de données sensibles de Macie avec Amazon Athena et QuickSight Amazon AWS sur le blog de sécurité.
> Pour obtenir des exemples de requêtes Athena que vous pouvez utiliser pour analyser les résultats de découverte de données sensibles, consultez le référentiel Amazon Macie Results Analytics sur. GitHub Ce référentiel fournit également des instructions pour configurer Athena

afin de récupérer et de déchiffrer vos résultats, ainsi que des scripts pour créer des tables pour les résultats.

Notation de sensibilité pour les compartiments S3

Si la découverte automatique des données sensibles est activée, Amazon Macie calcule et attribue automatiquement un score de sensibilité à chaque compartiment à usage général Amazon Simple Storage Service (Amazon S3) qu'il surveille et analyse pour un compte ou une organisation. Un score de sensibilité est une représentation quantitative de la quantité de données sensibles qu'un compartiment S3 peut contenir. Sur la base de ce score, Macie attribue également une étiquette de sensibilité à chaque seau. Une étiquette de sensibilité est une représentation qualitative du score de sensibilité d'un compartiment. Ces valeurs peuvent servir de points de référence pour déterminer où les données sensibles peuvent se trouver dans votre patrimoine de données Amazon S3, ainsi que pour identifier et surveiller les risques de sécurité potentiels liés à ces données.

Par défaut, le score de sensibilité et l'étiquette d'un compartiment S3 reflètent les résultats des activités automatisées de découverte de données sensibles que Macie a effectuées jusqu'à présent pour le compartiment. Ils ne reflètent pas les résultats des tâches de découverte de données sensibles que vous avez créées et exécutées. En outre, ni le score ni le label n'impliquent ou n'indiquent de quelque manière que ce soit la criticité ou l'importance qu'un bucket ou les objets d'un bucket peuvent avoir pour votre organisation. Cependant, vous pouvez annuler le score calculé d'un compartiment en attribuant manuellement le score maximum (100) au compartiment, qui attribue également le label Sensitive au compartiment.

Rubriques

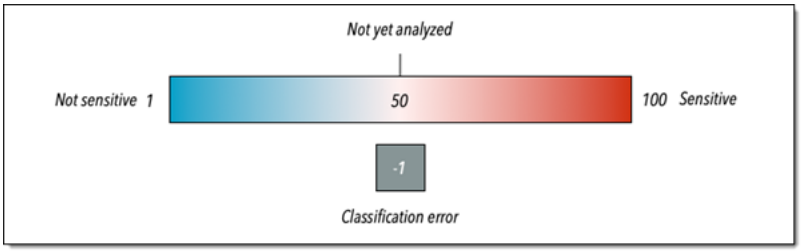
Dimensions et plages de notation de sensibilité

S'il est calculé par Amazon Macie, le score de sensibilité d'un compartiment S3 est une mesure quantitative de l'intersection de deux dimensions principales :

- La quantité de données sensibles que Macie a trouvées dans le compartiment. Cela tient principalement à la nature et au nombre de types de données sensibles que Macie a trouvés dans le compartiment et au nombre d'occurrences de chaque type.

- La quantité de données que Macie a analysées dans le compartiment. Cela provient principalement du nombre d'objets uniques analysés par Macie dans le compartiment par rapport au nombre total d'objets uniques dans le compartiment.

Le score de sensibilité d'un compartiment S3 détermine également l'étiquette de sensibilité que Macie attribue au compartiment. L'étiquette de sensibilité est une représentation qualitative du score, par exemple, Sensible ou Non sensible. Sur la console Amazon Macie, le score de sensibilité d'un bucket détermine également la couleur que Macie utilise pour représenter le bucket dans les visualisations de données, comme le montre l'image suivante.



Les scores de sensibilité vont de -1 à 100, comme décrit dans le tableau suivant. Pour évaluer les entrées dans le score d'un compartiment S3, vous pouvez vous référer aux statistiques de découverte de données sensibles et aux autres informations fournies par Macie à propos du compartiment.

Score de sensibilité	Étiquette de sensibilité	Informations supplémentaires
-1	Erreur de classification	Macie n'a encore réussi à analyser aucun des objets du compartiment en raison d'erreurs de classification au niveau des objets (problème s liés aux paramètres des autorisations au niveau des objets, au contenu des objets ou aux quotas). Lorsque Macie a essayé d'analyser un ou plusieurs objets du compartiment, des erreurs se sont produites.

Score de sensibilité	Étiquette de sensibilité	Informations supplémentaires
		Par exemple, un objet est un fichier mal formé ou un objet est chiffré avec une clé à laquelle Macie ne peut pas accéder ou n'est pas autorisée à utiliser. Les données de couverture du compartiment peuvent vous aider à étudier et à corriger les erreurs. Pour plus d'informations, consultez Évaluation de la couverture de la découverte automatique des données sensibles. Macie continuera d'essayer d'analyser les objets contenus dans le compartiment. Si Macie analyse un objet avec succès, Macie mettra à jour le score de sensibilité et l'étiquette du bucket pour refléter les résultats de l'analyse.

Score de sensibilité	Étiquette de sensibilité	Informations supplémentaires
1-49	Non sensible	Dans cette fourchette, un score plus élevé, 49 par exemple, indique que Macie a analysé relativement peu d'objets dans le compartiment. Un score inférieur, tel que 1, indique que Macie a analysé de nombreux objets du compartiment (par rapport au nombre total d'objets contenus dans le compartiment) et a détecté relativement peu de types et d'occurrences de données sensibles dans ces objets. Un score de 1 peut également indiquer que le compartiment ne stocke aucun objet ou que tous les objets du compartiment contiennent zéro (0) octet de données. Les statistiques relatives aux objets figurant dans les détails du compartiment peuvent vous aider à déterminer si tel est le cas. Pour plus d'informations, consultez Consulter les détails du bucket S3.

Score de sensibilité	Étiquette de sensibilité	Informations supplémentaires
50	Pas encore analysé	Macie n'a pas encore essayé d'analyser ou d'analyse r aucun des objets du compartiment. Macie attribue automatiq uement ce score lorsque la découverte automatique est initialement activée ou qu'un compartiment est ajouté à l'inventaire des compartim ents d'un compte. Dans une organisation, un bucket peut également avoir ce score si la découverte automatique n'a jamais été activée pour le compte propriétaire du bucket. Un score de 50 peut également indiquer que les paramètres d'autorisation du bucket empêchent Macie d'accéder au bucket ou aux objets du bucket. Cela est généralement dû à une politique de compartiment restrictive. Les détails du bucket peuvent vous aider à déterminer si c'est le cas, car Macie ne peut fournir qu'un sous-ensemble d'informa tions sur le bucket. Pour plus d'informations sur la manière de résoudre ce problème, consultezAutoriser Macie à

Score de sensibilité	Étiquette de sensibilité	Informations supplémentaires
		accéder aux compartiments et aux objets S3.
51-99	Sensible	Dans cette fourchette, un score plus élevé, tel que 99, indique que Macie a analysé de nombreux objets du compartiment (par rapport au nombre total d'objets contenus dans le compartiment) et détecté de nombreux types et occurrences de données sensibles dans ces objets. Un score inférieur, tel que 51, indique que Macie a analysé un nombre modéré d'objets dans le compartiment (par rapport au nombre total d'objets dans le compartiment) et détecté au moins quelques types et occurrences de données sensibles dans ces objets.
100	Sensible	Le score a été attribué manuellement au compartiment, remplaçant le score calculé. Macie n'attribue pas ce score aux buckets.

Surveillance des scores de sensibilité

Lorsque la découverte automatique des données sensibles est initialement activée pour un compte, Amazon Macie attribue automatiquement un score de sensibilité de 50 à chaque compartiment S3 détenu par le compte. Macie attribue également ce score à un compartiment lorsque celui-ci est

ajouté à l'inventaire des compartiments d'un compte. Sur la base de ce score, l'étiquette de sensibilité de chaque seau n'est pas encore analysée. L'exception est un compartiment vide, c'est-à-dire un compartiment qui ne stocke aucun objet ou dans lequel tous les objets du compartiment contiennent zéro (0) octet de données. Si tel est le cas pour un bucket, Macie attribue un score de 1 au bucket et l'étiquette de sensibilité du bucket est Non sensible.

Au fur et à mesure que la découverte automatique des données sensibles progresse chaque jour, Macie met à jour les scores de sensibilité et les étiquettes des compartiments S3 afin de refléter les résultats de son analyse. Par exemple :

- Si Macie ne trouve aucune donnée sensible dans un objet, Macie diminue le score de sensibilité du compartiment et met à jour l'étiquette de sensibilité du compartiment si nécessaire.
- Si Macie trouve des données sensibles dans un objet, Macie augmente le score de sensibilité du compartiment et met à jour l'étiquette de sensibilité du compartiment si nécessaire.
- Si Macie trouve des données sensibles dans un objet qui est ensuite modifié, Macie supprime les données sensibles détectées pour l'objet du score de sensibilité du compartiment et met à jour l'étiquette de sensibilité du compartiment si nécessaire.
- Si Macie trouve des données sensibles dans un objet qui est ensuite supprimé, Macie supprime les données sensibles détectées pour l'objet du score de sensibilité du compartiment et met à jour l'étiquette de sensibilité du compartiment si nécessaire.
- Si un objet est ajouté à un compartiment qui était auparavant vide et que Macie trouve des données sensibles dans l'objet, Macie augmente le score de sensibilité du compartiment et met à jour l'étiquette de sensibilité du compartiment si nécessaire.
- Si les paramètres d'autorisation d'un bucket empêchent Macie de récupérer des informations sur le bucket ou les objets du bucket ou d'y accéder, Macie modifie le score de sensibilité du bucket à 50 et change l'étiquette de sensibilité du bucket à Non encore analysé.

Les résultats d'analyse peuvent commencer à apparaître dans les 48 heures suivant l'activation de la découverte automatique des données sensibles pour un compte.

Si vous êtes l'administrateur Macie d'une organisation ou si vous possédez un compte Macie autonome, vous pouvez ajuster les paramètres de score de sensibilité de votre organisation ou de votre compte :

- Pour ajuster les paramètres pour les analyses ultérieures de tous les compartiments S3, modifiez les paramètres de découverte automatique des données sensibles de votre compte. Vous pouvez commencer à inclure ou à exclure des identifiants de données gérés spécifiques, des

identifiants de données personnalisés ou des listes d'autorisation. Vous pouvez également exclure des buckets spécifiques. Pour plus d'informations, consultez Configuration de la découverte automatique.

- Pour ajuster les paramètres des compartiments S3 individuels, modifiez les paramètres de découverte automatique des données sensibles pour chaque compartiment. Vous pouvez inclure ou exclure des types spécifiques de données sensibles du score d'un bucket. Vous pouvez également spécifier s'il convient d'attribuer un score calculé automatiquement à un bucket. Pour plus d'informations, consultez Gestion de la découverte automatique pour des compartiments S3 individuels.

Si vous désactivez la découverte automatique des données sensibles, l'effet sur les scores de sensibilité et les étiquettes existants varie. Si vous le désactivez pour le compte d'un membre d'une organisation, les scores et étiquettes existants sont conservés pour les compartiments S3 détenus par le compte. Si vous le désactivez pour l'ensemble d'une organisation ou pour un compte Macie autonome, les scores et labels existants ne sont conservés que pendant 30 jours. Au bout de 30 jours, Macie réinitialise les scores et les étiquettes pour tous les compartiments détenus par l'organisation ou le compte. Si un compartiment contient des objets, Macie change le score à 50 et attribue le label Pas encore analysé au compartiment. Si un compartiment est vide, Macie change le score à 1 et attribue le label Non sensible au compartiment. Après cette réinitialisation, Macie arrête de mettre à jour les scores de sensibilité et les étiquettes des compartiments, sauf si vous réactivez la découverte automatique des données sensibles pour l'organisation ou le compte.

Paramètres par défaut pour la découverte automatique des données sensibles

Si la découverte automatique des données sensibles est activée, Amazon Macie sélectionne et analyse automatiquement des exemples d'objets provenant de tous les compartiments à usage général Amazon Simple Storage Service (Amazon S3) qu'il surveille et analyse pour votre compte. Si vous êtes l'administrateur Macie d'une organisation, cela inclut par défaut les compartiments S3 que possèdent vos comptes membres.

Pour affiner la portée des analyses, vous pouvez exclure des compartiments S3 spécifiques de la découverte automatique de données sensibles. Vous pouvez le faire de deux manières : en modifiant les paramètres de votre compte et en modifiant les paramètres des compartiments individuels. Si vous êtes administrateur Macie, vous pouvez également activer ou désactiver la découverte automatique des données sensibles pour les comptes individuels de votre organisation. Pour plus d'informations, consultez Configuration de la découverte automatique des données sensibles.

Par défaut, Macie analyse les objets S3 en utilisant uniquement l'ensemble d'identifiants de données gérés que nous recommandons pour la découverte automatique des données sensibles. Macie n'utilise aucun identifiant de données personnalisé ni n'autorise les listes que vous avez définies. Pour personnaliser les analyses, vous pouvez configurer Macie pour utiliser des identifiants de données gérés spécifiques, des identifiants de données personnalisés et des listes d'autorisations. Vous pouvez le faire en modifiant les paramètres de votre compte. Pour plus d'informations, consultez Configuration de la découverte automatique des données sensibles.

Rubriques

- Identifiants de données gérés par défaut pour la découverte automatique des données sensibles
- Mises à jour des paramètres par défaut pour la découverte automatique des données sensibles

Identifiants de données gérés par défaut pour la découverte automatique des données sensibles

Par défaut, Amazon Macie analyse les objets S3 en utilisant uniquement l'ensemble d'identifiants de données gérés que nous recommandons pour la découverte automatique de données sensibles. Cet ensemble par défaut d'identifiants de données gérées est conçu pour détecter les catégories et types courants de données sensibles. Sur la base de nos recherches, il peut détecter les catégories générales et les types de données sensibles tout en optimisant les résultats de vos découvertes automatisées en réduisant le bruit.

L'ensemble par défaut est dynamique. Lorsque nous publions de nouveaux identifiants de données gérées, nous les ajoutons à l'ensemble par défaut s'ils sont susceptibles d'optimiser davantage les résultats de votre découverte automatisée de données sensibles. Au fil du temps, nous pouvons également ajouter ou supprimer des identifiants de données gérées existants de l'ensemble. La suppression d'un identifiant de données géré n'affecte pas les statistiques de découverte de données sensibles existantes ni les détails relatifs à vos compartiments S3. Par exemple, si nous supprimons l'identifiant de données gérées pour un type de données sensibles que Macie a précédemment détectées dans un bucket, Macie continue de signaler ces détections pour le bucket. Si nous ajoutons ou supprimons un identifiant de données gérées dans l'ensemble par défaut, nous mettons à jour cette page pour indiquer la nature et le moment de la modification. Pour recevoir des alertes automatiques concernant ces modifications, vous pouvez vous abonner au flux RSS sur la page d'historique des documents Macie.

Les rubriques suivantes répertorient les identificateurs de données gérés actuellement dans l'ensemble par défaut, organisés par catégorie et type de données sensibles. Ils spécifient l'identifiant

unique (ID) pour chaque identifiant de données gérées de l'ensemble. Cet identifiant décrit le type de données sensibles qu'un identifiant de données géré est conçu pour détecter, par exemple : `PGP_PRIVATE_KEY` pour les clés privées PGP et `USA_PASSPORT_NUMBER` pour les numéros de passeport américains. Si vous modifiez les paramètres de découverte automatique des données sensibles de votre compte, vous pouvez utiliser cet identifiant pour exclure explicitement un identifiant de données gérées des analyses ultérieures.

Rubriques

- Informations d'identification
- Informations financières
- données d'identification personnelle (PII)

Pour plus de détails sur les identifiants de données gérées spécifiques ou pour une liste complète de tous les identifiants de données gérées actuellement fournis par Macie, consultez. Utilisation des identificateurs de données gérés

Informations d'identification

Pour détecter les occurrences de données d'identification dans les objets S3, Macie utilise par défaut les identifiants de données gérés suivants.

Type de données sensibles	ID d'identifiant de données géré
AWS clé d'accès secrète	`AWS_CREDENTIALS`
En-tête d'autorisation HTTP Basic	`HTTP_BASIC_AUTH_HEADER`
Clé privée OpenSSH	`OPENSSH_PRIVATE_KEY`
Clé privée PGP	`PGP_PRIVATE_KEY`
Clé privée selon la norme PKCS (Public Key Cryptography Standard)	`PKCS`
Clé privée PuTTY	`PUTTY_PRIVATE_KEY`

Informations financières

Pour détecter les occurrences d'informations financières dans les objets S3, Macie utilise par défaut les identifiants de données gérés suivants.

Type de données sensibles	ID d'identifiant de données géré
Données sur la bande magnétique des cartes de crédit	`CREDIT_CARD_MAGNETIC_STRIPE`
Numéro de carte de crédit	`CREDIT_CARD_NUMBER` (pour les numéros de carte de crédit situés à proximité d'un mot clé)

données d'identification personnelle (PII)

Pour détecter les occurrences d'informations personnelles identifiables (PII) dans les objets S3, Macie utilise par défaut les identifiants de données gérés suivants.

Type de données sensibles	ID d'identifiant de données géré
Numéro d'identification du permis de conduire	`CANADA_DRIVERS_LICENSE`, `DRIVERS_LICENSE` (pour les États-Unis), `UK_DRIVERS_LICENSE`
Numéro de liste électorale	`UK_ELECTORAL_ROLL_NUMBER`
Numéro d'identification nationale	`FRANCE_NATIONAL_IDENTIFICATION_NUMBER`, `GERMANY_NATIONAL_IDENTIFICATION_NUMBER`, `ITALY_NATIONAL_IDENTIFICATION_NUMBER`, `SPAIN_DNI_NUMBER`
Numéro d'assurance nationale (NINO)	`UK_NATIONAL_INSURANCE_NUMBER`
Numéro de passeport	`CANADA_PASSPORT_NUMBER`, `FRANCE_PASSPORT_NUMBER`, `GERMANY_PASSPORT_NUMBER`, `ITALY_PAS`

Type de données sensibles	ID d'identifiant de données géré
	SPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER
Numéro de sécurité sociale	CANADA_SOCIAL_INSURANCE_NUMBER
Numéro de sécurité sociale	SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER
Numéro d'identification ou de référence du contribuable	AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER

Mises à jour des paramètres par défaut pour la découverte automatique des données sensibles

Le tableau suivant décrit les modifications apportées aux paramètres qu'Amazon Macie utilise par défaut pour la découverte automatique des données sensibles. Pour recevoir des alertes automatiques concernant ces modifications, abonnez-vous au flux RSS sur la page d'historique des documents Macie.

Modification	Description	Date
Implémentation d'un nouvel ensemble dynamique d'identifiants de données gérés par défaut	Les nouvelles configurations de découverte automatique des données sensibles sont désormais basées sur un ensemble dynamique par défaut d'identifiants	02/08/2023

Modification	Description	Date
	de données gérées. Si vous activez la découverte automatique des données sensibles pour la première fois à cette date ou après cette date, votre configura tion est basée sur l'ensemble dynamique. Si vous avez activé la découverte automatique des données sensibles pour la première fois avant cette date, votre configuration est basée sur un ensemble différent d'identifiants de données gérées. Pour plus d'informa tions, consultez les notes après ce tableau.	
Disponibilité générale	Première version de la découverte automatique des données sensibles.	28 novembre 2022

Si vous avez initialement activé la découverte automatique des données sensibles avant le 2 août 2023, votre configuration n'est pas basée sur l'ensemble dynamique d'identifiants de données gérées par défaut. Il est plutôt basé sur un ensemble statique d'identifiants de données gérées que nous avons définis pour la version initiale de la découverte automatique des données sensibles, comme indiqué dans le tableau ci-dessous.

Pour déterminer à quel moment vous avez initialement activé la découverte automatique des données sensibles, choisissez Découverte automatique des données sensibles dans le volet de navigation de la console Amazon Macie, puis reportez-vous à la date d'activation dans la section État. Pour ce faire par programmation, utilisez le GetAutomatedDiscoveryConfigurationfonctionnement de l'API Amazon Macie et reportez-vous à la

valeur du champ. `firstEnabledAt` Si la date est antérieure au 2 août 2023 et que vous souhaitez commencer à utiliser l'ensemble dynamique d'identifiants de données gérés par défaut, contactez AWS Support pour obtenir de l'aide.

Le tableau suivant répertorie tous les identificateurs de données gérées figurant dans l'ensemble statique. Le tableau est d'abord trié par catégorie de données sensibles, puis par type de données sensibles. Pour plus de détails sur les identifiants de données gérés spécifiques, consultezUtilisation des identificateurs de données gérés.

Catégorie de données sensibles	Type de données sensibles	ID d'identifiant de données géré
Informations d'identification	AWS clé d'accès secrète	`AWS_CREDENTIALS`
Informations d'identification	En-tête d'autorisation HTTP Basic	`HTTP_BASIC_AUTH_HEADER`
Informations d'identification	Clé privée OpenSSH	`OPENSSH_PRIVATE_KEY`
Informations d'identification	Clé privée PGP	`PGP_PRIVATE_KEY`
Informations d'identification	Clé privée selon la norme PKCS (Public Key Cryptography Standard)	`PKCS`
Informations d'identification	Clé privée PuTTY	`PUTTY_PRIVATE_KEY`
Informations financières	Numéro de compte bancaire	`BANK_ACCOUNT_NUMBER` (pour les numéros de comptes bancaires canadiens et américains), `FRANCE_BANK_ACCOUNT_NUMBER`, `GERMANY_BANK_ACCOUNT_NUMBER`, `ITALY_BANK_ACCOUNT_NUMBER`, `SPAIN_BANK_ACCOUNT_NUMBER`, `UK_BANK_ACCOUNT_NUMBER`

Catégorie de données sensibles	Type de données sensibles	ID d'identifiant de données géré
Informations financières	Date d'expiration de carte de crédit	`CREDIT_CARD_EXPIRATION`
Informations financières	Données sur la bande magnétique des cartes de crédit	`CREDIT_CARD_MAGNETIC_STRIPE`
Informations financières	Numéro de carte de crédit	`CREDIT_CARD_NUMBER` (pour les numéros de carte de crédit situés à proximité d'un mot clé)
Informations financières	Code de vérification de carte de crédit	`CREDIT_CARD_SECURITY_CODE`
Informations personnelles : Informations médicales personnelles (PHI)	Numéro d'enregistrement de DEA (Drug Enforcement Agency)	`US_DRUG_ENFORCEMENT_AGENCY_NUMBER`
Informations personnelles : PHI	Numéro de règlement de sécurité sociale (HICN)	`USA_HEALTH_INSURANCE_CLAIM_NUMBER`
Informations personnelles : PHI	Numéro d'assurance maladie ou d'identification médicale	`CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER`

Catégorie de données sensibles	Type de données sensibles	ID d'identifiant de données géré
Informations personnelles : PHI	Code du système de codage des procédures communes pour les soins de santé (HCPCS)	`USA_HEALTHCARE_PROCEDURE_CODE`
Informations personnelles : PHI	Code national des médicaments (NCD)	`USA_NATIONAL_DRUG_CODE`
Informations personnelles : PHI	Identifiant de fournisseur national (NPI)	`USA_NATIONAL_PROVIDER_IDENTIFIER`
Informations personnelles : PHI	Identifiant unique de l'appareil (UDI)	`MEDICAL_DEVICE_UDI`
Informations personnelles : informations personnelles identifiables (PII)	Date de naissance	`DATE_OF_BIRTH`

Catégorie de données sensibles	Type de données sensibles	ID d'identifiant de données géré
Informations personnelles : PII	Numéro d'identification du permis de conduire	`AUSTRALIA_DRIVERS_LICENSE`, `AUSTRIA_DRIVERS_LICENSE`, `BELGIUM_DRIVERS_LICENSE`, `BULGARIA_DRIVERS_LICENSE`, `CANADA_DRIVERS_LICENSE`, `CROATIA_DRIVERS_LICENSE`, `CYPRUS_DRIVERS_LICENSE`, `CZECHIA_DRIVERS_LICENSE`, `DENMARK_DRIVERS_LICENSE`, `DRIVERS_LICENSE` (pour les États-Unis), `ESTONIA_DRIVERS_LICENSE`, `FINLAND_DRIVERS_LICENSE`, `FRANCE_DRIVERS_LICENSE`, `GERMANY_DRIVERS_LICENSE`, `GREECE_DRIVERS_LICENSE`, `HUNGARY_DRIVERS_LICENSE`, `IRELAND_DRIVERS_LICENSE`, `ITALY_DRIVERS_LICENSE`, `LATVIA_DRIVERS_LICENSE`, `LITHUANIA_DRIVERS_LICENSE`, `LUXEMBOURG_DRIVERS_LICENSE`, `MALTA_DRIVERS_LICENSE`,

Catégorie de données sensibles	Type de données sensibles	ID d'identifiant de données géré
		NETHERLANDS_DRIVERS_LICENSE, POLAND_DRIVERS_LICENSE, PORTUGAL_DRIVERS_LICENSE, ROMANIA_DRIVERS_LICENSE, SLOVAKIA_DRIVERS_LICENSE, SLOVENIA_DRIVERS_LICENSE, SPAIN_DRIVERS_LICENSE, SWEDEN_DRIVERS_LICENSE, UK_DRIVERS_LICENSE
Informations personnelles : PII	Numéro de liste électorale	UK_ELECTORAL_ROLL_NUMBER
Informations personnelles : PII	Nom complet	NAME
Informations personnelles : PII	Coordonnées du système de positionnement mondial (GPS)	LATITUDE_LONGITUDE
Informations personnelles : PII	Adresse postale	ADDRESS, BRAZIL_CEP_CODE
Informations personnelles : PII	Numéro d'identification nationale	BRAZIL_RG_NUMBER, FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER

Catégorie de données sensibles	Type de données sensibles	ID d'identifiant de données géré
Informations personnelles : PII	Numéro d'assurance nationale (NINO)	`UK_NATIONAL_INSURANCE_NUMBER`
Informations personnelles : PII	Numéro de passeport	`CANADA_PASSPORT_NUMBER`, `FRANCE_PASSPORT_NUMBER`, `GERMANY_PASSPORT_NUMBER`, `ITALY_PASSPORT_NUMBER`, `SPAIN_PASSPORT_NUMBER`, `UK_PASSPORT_NUMBER`, `USA_PASSPORT_NUMBER`
Informations personnelles : PII	Numéro de résidence permanente	`CANADA_NATIONAL_IDENTIFICATION_NUMBER`
Informations personnelles : PII	Phone number (Numéro de téléphone)	`BRAZIL_PHONE_NUMBER`, `FRANCE_PHONE_NUMBER`, `GERMANY_PHONE_NUMBER`, `ITALY_PHONE_NUMBER`, `PHONE_NUMBER` (pour le Canada et les États-Unis), `SPAIN_PHONE_NUMBER`, `UK_PHONE_NUMBER`
Informations personnelles : PII	Numéro de sécurité sociale	`CANADA_SOCIAL_INSURANCE_NUMBER`
Informations personnelles : PII	Numéro de sécurité sociale	`SPAIN_SOCIAL_SECURITY_NUMBER`, `USA_SOCIAL_SECURITY_NUMBER`

Catégorie de données sensibles	Type de données sensibles	ID d’identifiant de données géré
Informations personnelles : PII	Numéro d'identification ou de référence du contribuable	`AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER`
Informations personnelles : PII	Numéro d’identification de véhicule (VIN)	`VEHICLE_IDENTIFICATION_NUMBER`

Exécution de tâches de découverte de données sensibles dans Amazon Macie

Avec Amazon Macie, vous pouvez créer et exécuter des tâches de découverte de données sensibles afin d'automatiser la découverte, la journalisation et le reporting des données sensibles dans les compartiments à usage général Amazon Simple Storage Service (Amazon S3). Une tâche de découverte de données sensibles est une série de tâches de traitement et d'analyse automatisées que Macie exécute pour détecter et signaler les données sensibles dans les objets Amazon S3. Chaque tâche fournit des rapports détaillés sur les données sensibles trouvées par Macie et sur les analyses effectuées par Macie. En créant et en exécutant des tâches, vous pouvez créer et gérer une vue complète des données que votre organisation stocke dans Amazon S3 et des risques de sécurité ou de conformité associés à ces données.

Pour vous aider à respecter et à maintenir la conformité à vos exigences en matière de sécurité et de confidentialité des données, Macie propose plusieurs options pour planifier et définir l'étendue d'une tâche. Vous pouvez configurer une tâche pour qu'elle ne soit exécutée qu'une seule fois pour une analyse et une évaluation à la demande, ou de manière récurrente pour une analyse, une évaluation et une surveillance périodiques. Vous définissez également l'étendue et la profondeur de l'analyse d'une tâche, qu'il s'agisse de compartiments S3 spécifiques que vous sélectionnez ou de compartiments répondant à des critères spécifiques. Vous pouvez éventuellement affiner la portée de cette analyse en choisissant des options supplémentaires. Les options incluent des critères d'inclusion et d'exclusion personnalisés qui découlent des propriétés des objets S3, tels que les balises, les préfixes et la date de dernière modification d'un objet.

Pour chaque tâche, vous spécifiez également les types de données sensibles que vous souhaitez que Macie détecte et signale. Vous pouvez configurer une tâche pour utiliser les identifiants de données gérés fournis par Macie, les identifiants de données personnalisés que vous définissez ou une combinaison des deux. En sélectionnant des identifiants de données gérés et personnalisés spécifiques pour une tâche, vous pouvez adapter l'analyse pour qu'elle se concentre sur des types spécifiques de données sensibles. Pour affiner l'analyse, vous pouvez également configurer une tâche afin d'utiliser les listes d'autorisation que vous définissez. Les listes d'autorisations spécifient le texte et les modèles de texte que vous souhaitez que Macie ignore, généralement des exceptions de données sensibles pour les scénarios ou l'environnement particuliers de votre organisation.

Chaque tâche produit des enregistrements des données sensibles trouvées par Macie et des analyses effectuées par Macie, c'est-à-dire les découvertes de données sensibles et les résultats de découverte de données sensibles. Une découverte de données sensibles est un rapport détaillé des données sensibles que Macie a trouvées dans un objet S3. Un résultat de découverte de données sensibles est un enregistrement qui enregistre les détails de l'analyse d'un objet S3. Macie crée un résultat de découverte de données sensibles pour chaque objet que vous configurez une tâche à analyser. Cela inclut les objets dans lesquels Macie ne trouve pas de données sensibles et ne produisent donc pas de données sensibles, ainsi que les objets que Macie ne peut pas analyser en raison d'erreurs ou de problèmes. Chaque type d'enregistrement adhère à un schéma standardisé, qui peut vous aider à interroger, surveiller et traiter les enregistrements afin de répondre à vos exigences de sécurité et de conformité.

Rubriques

- Surveillance des tâches de découverte de données sensibles avec Amazon CloudWatch Logs
- Gestion des tâches de découverte de données sensibles
- Prédiction et surveillance des coûts pour les tâches de découverte de données sensibles
- Identificateurs de données gérés recommandés pour les tâches de découverte de données sensibles

Options d'étendue pour les tâches de découverte de données sensibles

Avec les tâches de découverte de données sensibles, vous définissez l'étendue des données Amazon Simple Storage Service (Amazon S3) qu'Amazon Macie analyse pour détecter et signaler les données sensibles. Pour vous aider à le faire, Macie propose plusieurs options spécifiques à la tâche que vous pouvez choisir lorsque vous créez et configurez une tâche.

Options de portée

- Compartiments S3
- Exécution initiale : objets S3 existants
- Profondeur d'échantillonnage
- Critères relatifs aux objets S3

Compartiments S3

Lorsque vous créez une tâche de découverte de données sensibles, vous spécifiez les compartiments S3 qui stockent les objets que vous souhaitez que Macie analyse lors de l'exécution de la tâche. Vous pouvez le faire de deux manières : en sélectionnant des compartiments S3 spécifiques dans votre inventaire de compartiments ou en spécifiant des critères personnalisés dérivés des propriétés des compartiments S3.

Sélectionnez des compartiments S3 spécifiques

> Avec cette option, vous sélectionnez explicitement chaque compartiment S3 à analyser. Ensuite, lorsque la tâche s'exécute, elle analyse les objets uniquement dans les compartiments que vous sélectionnez. Si vous configurez une tâche pour qu'elle s'exécute régulièrement sur une base quotidienne, hebdomadaire ou mensuelle, la tâche analyse les objets contenus dans ces mêmes compartiments à chaque exécution.

Cette configuration est utile lorsque vous souhaitez effectuer une analyse ciblée d'un ensemble de données spécifique. Il vous permet de contrôler de manière précise et prévisible les catégories analysées par un poste.

Spécifier les critères du compartiment S3

Avec cette option, vous définissez des critères d'exécution qui déterminent les compartiments S3 à analyser. Les critères consistent en une ou plusieurs conditions dérivées des propriétés du compartiment, telles que les paramètres d'accès public et les balises. Lorsque la tâche est exécutée, elle identifie les compartiments correspondant à vos critères, puis analyse les objets qu'ils contiennent. Si vous configurez une tâche pour qu'elle s'exécute régulièrement, elle le fait à chaque fois qu'elle s'exécute. Par conséquent, la tâche peut analyser des objets dans différents compartiments à chaque exécution, en fonction des modifications apportées à votre inventaire de compartiments et des critères que vous définissez.

Cette configuration est utile dans les cas où vous souhaitez que l'étendue de l'analyse s'adapte de manière dynamique aux modifications apportées à votre inventaire de compartiments. Si vous configurez une tâche pour utiliser des critères de compartiment et qu'elle est exécutée régulièrement, la tâche identifie automatiquement les nouveaux compartiments qui répondent aux critères et inspecte ces compartiments pour détecter la présence de données sensibles.

Les rubriques de cette section fournissent des informations supplémentaires sur chaque option.

Rubriques

- Sélection de compartiments S3 spécifiques
- Spécification des critères du compartiment S3

Sélection de compartiments S3 spécifiques

Si vous choisissez de sélectionner explicitement chaque compartiment S3 que vous souhaitez qu'une tâche analyse, Macie vous fournit un inventaire complet de vos compartiments à usage général actuels. Région AWS Vous pouvez ensuite consulter votre inventaire et sélectionner les compartiments que vous souhaitez. Pour savoir comment Macie génère et gère cet inventaire pour vous, consultezComment Macie surveille la sécurité des données Amazon S3.

Si vous êtes l'administrateur Macie d'une organisation, l'inventaire inclut les buckets détenus par les comptes des membres de votre organisation. Vous pouvez sélectionner jusqu'à 1 000 de ces compartiments, couvrant jusqu'à 1 000 comptes.

Pour vous aider à sélectionner vos compartiments, l'inventaire fournit des détails et des statistiques pour chaque compartiment. Cela inclut la quantité de données que la tâche peut analyser dans chaque compartiment. Les objets classifiables sont des objets qui utilisent une classe de stockage Amazon S3 prise en charge et qui ont une extension de nom de fichier pour un format de fichier ou de stockage pris en charge. L'inventaire indique également si des tâches existantes sont configurées pour analyser les objets d'un compartiment. Ces informations peuvent vous aider à estimer l'étendue d'une tâche et à affiner vos sélections de compartiments.

Dans le tableau d'inventaire :

- Sensibilité : indique le score de sensibilité actuel d'un compartiment, si la découverte automatique des données sensibles est activée.
- Objets classifiables : indique le nombre total d'objets que la tâche peut analyser dans un compartiment.
- Taille classifiable : indique la taille de stockage totale de tous les objets que la tâche peut analyser dans un compartiment.

  Si un bucket stocke des objets compressés, cette valeur ne reflète pas la taille réelle de ces objets après leur décompression. Si le versionnement est activé pour un compartiment, cette valeur est basée sur la taille de stockage de la dernière version de chaque objet du compartiment.
- Surveillé par tâche : indique si des tâches existantes sont configurées pour analyser régulièrement les objets d'un bucket sur une base quotidienne, hebdomadaire ou mensuelle.

  Si la valeur de ce champ est Oui, le compartiment est explicitement inclus dans une tâche périodique ou le compartiment a répondu aux critères d'une tâche périodique au cours des dernières 24 heures. En outre, le statut d'au moins un de ces emplois n'est pas annulé. Macie met à jour ces données quotidiennement.
- Dernière exécution de la tâche : si des tâches périodiques ou ponctuelles existantes sont configurées pour analyser les objets d'un bucket, ce champ indique la date et l'heure les plus récentes auxquelles l'une de ces tâches a commencé à s'exécuter. Dans le cas contraire, un tiret (—) apparaît dans ce champ.

Si l'icône d'information
(ⓘ)
apparaît à côté d'un nom de compartiment dans le tableau, nous vous recommandons de récupérer les dernières métadonnées du compartiment sur Amazon S3. Pour ce faire, choisissez refresh

()
au-dessus du tableau. L'icône d'information indique qu'un bucket a été créé au cours des dernières 24 heures, probablement après que Macie ait récupéré pour la dernière fois les métadonnées du bucket et de l'objet sur Amazon S3 dans le cadre du cycle d'actualisation quotidien. Pour plus d'informations, consultez Actualisations de données.

Si l'icône d'avertissement
()
apparaît à côté du nom d'un bucket dans le tableau, Macie n'est pas autorisé à accéder au bucket ou aux objets du bucket. Cela signifie que la tâche ne sera pas en mesure d'analyser les objets du compartiment. Pour étudier le problème, consultez la politique du compartiment et les paramètres d'autorisation dans Amazon S3. Par exemple, le compartiment peut avoir une politique de compartiment restrictive. Pour plus d'informations, consultez Autoriser Macie à accéder aux compartiments et aux objets S3.

Pour personnaliser votre affichage de l'inventaire et trouver plus facilement des compartiments spécifiques, vous pouvez filtrer le tableau en saisissant des critères de filtre dans la zone de filtre. Le tableau suivant fournit quelques exemples.

Pour afficher tous les seaux qui...	Appliquer ce filtre...
Détenus par un compte spécifique	ID de compte = *l'identifiant à 12 chiffres du* compte
Sont accessibles au public	Autorisation effective = Publique
Ne sont inclus dans aucun emploi périodique	Surveillé activement par tâche = Faux
Ne sont inclus dans aucun travail périodique ou ponctuel	Défini dans le job = False
Disposer d'une clé de tag spécifique*	Clé de tag = *la clé de tag*
Avoir une valeur de tag spécifique*	Valeur du tag = *valeur du tag*
Stockez des objets non chiffrés (ou des objets utilisant le chiffrement côté client)	Le nombre d'objets par chiffrement est « Aucun chiffrement » et « From » = 1

* Les clés et les valeurs des balises distinguent les majuscules et minuscules. Vous devez également spécifier une valeur complète et valide pour ces champs dans un filtre. Vous ne pouvez pas spécifier de valeurs partielles ni utiliser de caractères génériques.

Pour afficher les détails d'un bucket, choisissez le nom du bucket et consultez le panneau des détails. À partir de là, vous pouvez également :

- Faites pivoter et explorez certains champs vers le bas en choisissant une loupe pour le champ. Choisissez
  
  d'afficher les compartiments avec la même valeur ou
  d' 
  affich
  les compartiments avec d'autres valeurs.
- Récupérez les dernières métadonnées pour les objets du compartiment. Cela peut être utile si vous avez récemment créé un bucket ou si vous avez apporté des modifications importantes aux objets du bucket au cours des dernières 24 heures. Pour récupérer les données, choisissez refresh
  (
)
  dans la section Statistiques des objets du panneau. Cette option est disponible pour les seaux contenant 30 000 objets ou moins.

Spécification des critères du compartiment S3

Si vous choisissez de définir des critères de compartiment pour une tâche, Macie propose des options permettant de définir et de tester les critères. Il s'agit de critères d'exécution qui déterminent quels compartiments S3 stockent les objets à analyser. Chaque fois que la tâche est exécutée, elle identifie les compartiments à usage général correspondant à vos critères, puis analyse les objets contenus dans les compartiments appropriés. Si vous êtes l'administrateur Macie d'une organisation, cela inclut les buckets détenus par les comptes des membres de votre organisation.

Définition des critères du bucket

Les critères de compartiment consistent en une ou plusieurs conditions dérivées des propriétés des compartiments S3. Chaque condition, également appelée critère, comprend les éléments suivants :

- Un champ basé sur des propriétés, tel que l'ID de compte ou l'autorisation effective.
- Un opérateur, égal à (`eq`) ou non égal (`neq`).
- Une ou plusieurs valeurs.

- Une instruction d'inclusion ou d'exclusion qui indique s'il faut analyser (inclure) ou ignorer (exclure) les compartiments correspondant à la condition.

Si vous spécifiez plusieurs valeurs pour un champ, Macie utilise la logique OR pour joindre les valeurs. Si vous spécifiez plusieurs conditions pour les critères, Macie utilise la logique AND pour joindre les conditions. En outre, les conditions d'exclusion ont priorité sur les conditions d'inclusion. Par exemple, si vous incluez des compartiments accessibles au public et que vous excluez les compartiments dotés de balises spécifiques, la tâche analyse les objets de tout compartiment accessible au public, sauf si le compartiment possède l'une des balises spécifiées.

Vous pouvez définir des conditions dérivées de l'un des champs de propriété suivants pour les compartiments S3.

ID de compte

Identifiant unique (ID) du propriétaire Compte AWS d'un compartiment. Pour spécifier plusieurs valeurs pour ce champ, entrez l'ID de chaque compte et séparez chaque entrée par une virgule.

Notez que Macie ne prend pas en charge l'utilisation de caractères génériques ou de valeurs partielles pour ce champ.

Nom du compartiment

Le nom d'un bucket. Ce champ est en corrélation avec le champ Name, et non avec le champ Amazon Resource Name (ARN), dans Amazon S3. Pour spécifier plusieurs valeurs pour ce champ, entrez le nom de chaque compartiment et séparez chaque entrée par une virgule.

Notez que les valeurs distinguent les majuscules et minuscules. De plus, Macie ne prend pas en charge l'utilisation de caractères génériques ou de valeurs partielles pour ce champ.

Autorisation effective

Spécifie si un compartiment est accessible au public. Vous pouvez choisir une ou plusieurs des valeurs suivantes pour ce champ :

- Non public : le grand public n'a pas accès au bucket en lecture ou en écriture.
- Public : le grand public dispose d'un accès en lecture ou en écriture au bucket.
- Inconnu : Macie n'a pas pu évaluer les paramètres d'accès public du bucket.

Pour déterminer cette valeur pour un bucket, Macie analyse une combinaison de paramètres au niveau du compte et du bucket pour le bucket : les paramètres de blocage de l'accès public pour

le compte ; les paramètres de blocage de l'accès public pour le bucket ; la politique du bucket ; et la liste de contrôle d'accès (ACL) du bucket.

Accès partagé

Spécifie si un compartiment est partagé avec un autre utilisateur Compte AWS, une identité CloudFront d'accès à l'origine (OAI) Amazon ou un contrôle CloudFront d'accès à l'origine (OAC). Vous pouvez choisir une ou plusieurs des valeurs suivantes pour ce champ :

- Externe : le bucket est partagé avec un ou plusieurs des éléments suivants ou une combinaison des éléments suivants : un CloudFront OAI, un CloudFront OAC ou un compte externe à votre organisation (n'en faisant pas partie).
- Interne : le bucket est partagé avec un ou plusieurs comptes internes à (une partie de) votre organisation. Il n'est pas partagé avec un CloudFront OAI ou un OAC.
- Non partagé : le bucket n'est pas partagé avec un autre compte, un CloudFront OAI ou un CloudFront OAC.
- Inconnu : Macie n'a pas pu évaluer les paramètres d'accès partagé pour le compartiment.

Pour déterminer si un bucket est partagé avec un autre Compte AWS, Macie analyse la politique de bucket et l'ACL du bucket. En outre, une organisation est définie comme un ensemble de comptes Macie gérés de manière centralisée en tant que groupe de comptes connexes via AWS Organizations ou sur invitation de Macie. Pour plus d'informations sur les options d'Amazon S3 pour le partage de compartiments, consultez la section Gestion des identités et des accès dans Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Pour déterminer si un bucket est partagé avec un CloudFront OAI ou un OAC, Macie analyse la politique de bucket applicable au bucket. Un CloudFront OAI ou un OAC permet aux utilisateurs d'accéder aux objets d'un bucket via une ou plusieurs distributions spécifiées CloudFront. Pour plus d'informations sur les CloudFront OAI et les OAC, consultez Restreindre l'accès à une origine Amazon S3 dans le manuel Amazon CloudFront Developer Guide.

Balises

Les balises associées à un bucket. Les balises sont des étiquettes que vous pouvez définir et attribuer à certains types de AWS ressources, notamment les compartiments S3. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Pour plus d'informations sur le balisage des compartiments S3, consultez la section Utilisation des balises de compartiment S3 pour la répartition des coûts dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Pour une tâche de découverte de données sensibles, vous pouvez utiliser ce type de condition pour inclure ou exclure des compartiments dotés d'une clé de balise spécifique, d'une valeur de balise spécifique ou d'une clé de balise et d'une valeur de balise spécifiques (par paire). Par exemple :

- Si vous spécifiez **`Project`** en tant que clé de balise et que vous ne spécifiez aucune valeur de balise pour une condition, tout compartiment contenant la clé de balise Project répond aux critères de la condition, quelles que soient les valeurs de balise associées à cette clé de balise.
- Si vous spécifiez **`Development`** et **`Test`** en tant que valeurs de balise et que vous ne spécifiez aucune clé de balise pour une condition, tout compartiment contenant la valeur de **`Test`** balise **`Development`** ou correspond aux critères de la condition, quelles que soient les clés de balise associées à ces valeurs de balise.

Pour spécifier plusieurs clés de balise dans une condition, entrez chaque clé de balise dans le champ Clé et séparez chaque entrée par une virgule. Pour spécifier plusieurs valeurs de balise dans une condition, entrez chaque valeur de balise dans le champ Valeur et séparez chaque entrée par une virgule.

Notez que les clés et les valeurs des balises distinguent les majuscules et minuscules. De plus, Macie ne prend pas en charge l'utilisation de caractères génériques ou de valeurs partielles dans les conditions des balises.

Critères du godet de test

Lorsque vous définissez les critères de votre compartiment, vous pouvez tester et affiner les critères en prévisualisant les résultats. Pour ce faire, développez la section Aperçu des résultats des critères qui apparaît sous les critères sur la console. Cette section affiche un tableau des compartiments S3 à usage général qui répondent actuellement aux critères.

Le tableau fournit également un aperçu de la quantité de données que la tâche peut analyser dans chaque compartiment. Les objets classifiables sont des objets qui utilisent une classe de stockage Amazon S3 prise en charge et qui ont une extension de nom de fichier pour un format de fichier ou de stockage pris en charge. Le tableau indique également si des tâches existantes sont configurées pour analyser périodiquement les objets d'un compartiment.

Dans le tableau :

- Sensibilité : indique le score de sensibilité actuel d'un compartiment, si la découverte automatique des données sensibles est activée.

- Objets classifiables : indique le nombre total d'objets que la tâche peut analyser dans un compartiment.
- Taille classifiable : indique la taille de stockage totale de tous les objets que la tâche peut analyser dans un compartiment.

  Si un bucket stocke des objets compressés, cette valeur ne reflète pas la taille réelle de ces objets après leur décompression. Si le versionnement est activé pour un compartiment, cette valeur est basée sur la taille de stockage de la dernière version de chaque objet du compartiment.
- Surveillé par tâche : indique si des tâches existantes sont configurées pour analyser régulièrement les objets d'un bucket sur une base quotidienne, hebdomadaire ou mensuelle.

  Si la valeur de ce champ est Oui, le compartiment est explicitement inclus dans une tâche périodique ou le compartiment a répondu aux critères d'une tâche périodique au cours des dernières 24 heures. En outre, le statut d'au moins un de ces emplois n'est pas annulé. Macie met à jour ces données quotidiennement.

Si l'icône d'avertissement
(⚠)
apparaît à côté du nom d'un bucket, Macie n'est pas autorisé à accéder au bucket ou aux objets du bucket. Cela signifie que la tâche ne sera pas en mesure d'analyser les objets du compartiment. Pour étudier le problème, consultez la politique du compartiment et les paramètres d'autorisation dans Amazon S3. Par exemple, le compartiment peut avoir une politique de compartiment restrictive. Pour plus d'informations, consultez Autoriser Macie à accéder aux compartiments et aux objets S3.

Pour affiner les critères du bucket pour la tâche, utilisez les options de filtre pour ajouter, modifier ou supprimer des conditions des critères. Macie met ensuite à jour le tableau pour refléter vos modifications.

Exécution initiale : objets S3 existants

Vous pouvez utiliser des tâches de découverte de données sensibles pour effectuer une analyse continue et incrémentielle des objets dans des compartiments S3. Si vous configurez une tâche pour qu'elle s'exécute régulièrement, Macie le fait automatiquement pour vous : chaque exécution analyse uniquement les objets créés ou modifiés après l'exécution précédente. Avec l'option Inclure les objets existants, vous choisissez le point de départ du premier incrément :

- Pour analyser tous les objets existants immédiatement après avoir créé la tâche, cochez la case correspondant à cette option.

- Pour attendre et analyser uniquement les objets créés ou modifiés après la création de la tâche et avant la première exécution, décochez la case correspondant à cette option.

  La désactivation de cette case à cocher est utile lorsque vous avez déjà analysé les données et que vous souhaitez continuer à les analyser régulièrement. Par exemple, si vous avez déjà utilisé un autre service ou une autre application pour classer les données et que vous avez récemment commencé à utiliser Macie, vous pouvez utiliser cette option pour garantir la découverte et la classification continues de vos données sans encourir de coûts inutiles ni dupliquer les données de classification.

Chaque exécution suivante d'une tâche périodique analyse automatiquement uniquement les objets créés ou modifiés après l'exécution précédente.

Pour les tâches périodiques et ponctuelles, vous pouvez également configurer une tâche pour analyser uniquement les objets créés ou modifiés avant ou après un certain temps ou pendant une certaine période. Pour ce faire, ajoutez des critères d'objet qui utilisent la date de dernière modification des objets.

Profondeur d'échantillonnage

Avec cette option, vous spécifiez le pourcentage d'objets S3 éligibles que vous souhaitez qu'une tâche de découverte de données sensibles analyse. Les objets éligibles sont les objets qui : utilisent une classe de stockage Amazon S3 prise en charge, ont une extension de nom de fichier pour un format de fichier ou de stockage pris en charge et répondent à d'autres critères que vous spécifiez pour la tâche.

Si cette valeur est inférieure à 100 %, Macie sélectionne les objets éligibles à analyser au hasard, jusqu'au pourcentage spécifié, et analyse toutes les données contenues dans ces objets. Par exemple, si vous configurez une tâche pour analyser 10 000 objets et que vous spécifiez une profondeur d'échantillonnage de 20 %, Macie analyse environ 2 000 objets éligibles sélectionnés au hasard lors de l'exécution de la tâche.

La réduction de la profondeur d'échantillonnage d'une tâche peut réduire le coût et la durée d'une tâche. C'est utile lorsque les données contenues dans les objets sont très cohérentes et que vous souhaitez déterminer si c'est un compartiment S3, plutôt que chaque objet, qui stocke des données sensibles.

Notez que cette option contrôle le pourcentage d'objets analysés, et non le pourcentage d'octets analysés. Si vous entrez une profondeur d'échantillonnage inférieure à 100 %, Macie analyse toutes

les données de chaque objet sélectionné, et non le pourcentage des données de chaque objet sélectionné.

Critères relatifs aux objets S3

Pour affiner l'étendue d'une tâche de découverte de données sensibles, vous pouvez également définir des critères personnalisés qui déterminent les objets S3 que Macie inclut ou exclut de l'analyse d'une tâche. Ces critères consistent en une ou plusieurs conditions dérivées des propriétés des objets S3. Les conditions s'appliquent aux objets de tous les compartiments S3 que vous configurez pour analyser une tâche. Si un bucket stocke plusieurs versions d'un objet, les conditions s'appliquent à la dernière version de l'objet.

Si vous définissez plusieurs conditions comme critères d'objet, Macie utilise la logique ET pour joindre les conditions. En outre, les conditions d'exclusion ont priorité sur les conditions d'inclusion. Par exemple, si vous incluez des objets portant l'extension de nom de fichier .pdf et que vous excluez des objets dont la taille est supérieure à 5 Mo, la tâche analyse tout objet portant l'extension de nom de fichier .pdf, sauf si l'objet est supérieur à 5 Mo.

Vous pouvez définir des conditions qui dérivent de l'une des propriétés suivantes des objets S3.

Extension de nom de fichier

Cela correspond à l'extension du nom de fichier d'un objet S3. Vous pouvez utiliser ce type de condition pour inclure ou exclure des objets en fonction du type de fichier. Pour ce faire pour plusieurs types de fichiers, entrez l'extension du nom de fichier pour chaque type et séparez chaque entrée par une virgule, par exemple :. **`docx,pdf,xlsx`** Si vous entrez plusieurs extensions de nom de fichier comme valeurs pour une condition, Macie utilise la logique OR pour joindre les valeurs.

Notez que les valeurs distinguent les majuscules et minuscules. De plus, Macie ne prend pas en charge l'utilisation de valeurs partielles ou de caractères génériques dans ce type de condition.

Pour plus d'informations sur les types de fichiers que Macie peut analyser, consultezFormats de fichiers et de stockage pris en charge.

Dernière modification

Cela correspond au champ Dernière modification dans Amazon S3. Dans Amazon S3, ce champ enregistre la date et l'heure de création ou de dernière modification d'un objet S3, selon la date la plus récente.

Pour une tâche de découverte de données sensibles, cette condition peut être une date précise, une date et une heure spécifiques ou une plage horaire exclusive :

- Pour analyser les objets qui ont été modifiés pour la dernière fois après une certaine date ou une certaine date et heure, entrez les valeurs dans les champs De.
- Pour analyser les objets qui ont été modifiés pour la dernière fois avant une certaine date ou date et heure, entrez les valeurs dans les champs À.
- Pour analyser les objets qui ont été modifiés pour la dernière fois pendant une certaine période, utilisez les champs From pour saisir les valeurs de la date ou de la première date et heure de la plage horaire. Utilisez les champs À pour saisir les valeurs de la dernière date ou de la dernière date et heure de la plage horaire.
- Pour analyser les objets qui ont été modifiés pour la dernière fois au cours d'une journée donnée, entrez la date dans le champ Date de début. Entrez la date du jour suivant dans le champ Date limite. Vérifiez ensuite que les deux champs temporels sont vides. (Macie traite un champ horaire vide comme`00:00:00`.) Par exemple, pour analyser des objets qui ont changé le 9 août 2023, entrez **`2023/08/09`** dans le champ Date de début, entrez **`2023/08/10`** dans le champ Date de fin et n'entrez de valeur dans aucun des champs temporels.

Entrez n'importe quelle valeur horaire en temps universel coordonné (UTC) et utilisez une notation de 24 heures.

Préfixe

Cela correspond au champ Key dans Amazon S3. Dans Amazon S3, ce champ stocke le nom d'un objet S3, y compris le préfixe de l'objet. Un préfixe est similaire à un chemin de répertoire dans un bucket. Il vous permet de regrouper des objets similaires dans un compartiment, de la même manière que vous stockiez des fichiers similaires dans un dossier d'un système de fichiers. Pour plus d'informations sur les préfixes d'objets et les dossiers dans Amazon S3, consultez la section Organisation des objets dans la console Amazon S3 à l'aide de dossiers dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Vous pouvez utiliser ce type de condition pour inclure ou exclure des objets dont les clés (noms) commencent par une certaine valeur. Par exemple, pour exclure tous les objets dont la clé commence par AWSLogs, entrez **`AWSLogs`** la valeur d'une condition de préfixe, puis choisissez Exclure.

Si vous entrez plusieurs préfixes comme valeurs pour une condition, Macie utilise la logique OR pour joindre les valeurs. Par exemple, si vous entrez **`AWSLogs1`** et **`AWSLogs2`** en tant que valeurs

pour une condition, tout objet dont la clé commence par AWSLogs1 ou AWSLogs2 correspond aux critères de la condition.

Lorsque vous entrez une valeur pour une condition de préfixe, gardez les points suivants à l'esprit :

- Les valeurs distinguent les majuscules et minuscules.
- Macie ne prend pas en charge l'utilisation de caractères génériques dans ces valeurs.
- Dans Amazon S3, la clé d'un objet n'inclut pas le nom du compartiment qui stocke l'objet. Pour cette raison, ne spécifiez pas de nom de compartiment dans ces valeurs.
- Si un préfixe inclut un délimiteur, incluez-le dans la valeur. Par exemple, entrez **`AWSLogs/eventlogs`** pour définir une condition pour tous les objets dont la clé commence par AWSLogs/eventlogs. Macie prend en charge le délimiteur Amazon S3 par défaut, qui est une barre oblique (/), et les délimiteurs personnalisés.

Notez également qu'un objet répond aux critères d'une condition uniquement si la clé de l'objet correspond exactement à la valeur que vous entrez, en commençant par le premier caractère de la clé de l'objet. En outre, Macie applique une condition à la valeur clé complète d'un objet, y compris le nom de fichier de l'objet.

Par exemple, si la clé d'un objet est AWSLogs/eventlogs/testlog.csv et que vous entrez l'une des valeurs suivantes pour une condition, l'objet répond aux critères de la condition :

- **`AWSLogs`**
- **`AWSLogs/event`**
- **`AWSLogs/eventlogs/`**
- **`AWSLogs/eventlogs/testlog`**
- **`AWSLogs/eventlogs/testlog.csv`**

Toutefois, si vous entrez***`eventlogs`***, l'objet ne correspond pas aux critères : la valeur de la condition n'inclut pas la première partie de la clé,/. AWSLogs De même, si vous entrez**`awslogs`**, l'objet ne correspond pas aux critères en raison de différences de capitalisation.

Taille de rangement

Cela correspond au champ Size dans Amazon S3. Dans Amazon S3, ce champ indique la taille de stockage totale d'un objet S3. Si un objet est un fichier compressé, cette valeur ne reflète pas la taille réelle du fichier une fois celui-ci décompressé.

Vous pouvez utiliser ce type de condition pour inclure ou exclure des objets inférieurs à une certaine taille, supérieurs à une certaine taille ou se situant dans une certaine plage de tailles. Macie applique ce type de condition à tous les types d'objets, y compris les fichiers compressés ou d'archive et les fichiers qu'ils contiennent. Pour plus d'informations sur les restrictions basées sur la taille pour chaque format pris en charge, consultezQuotas Amazon Macie.

Balises

Les balises associées à un objet S3. Les balises sont des étiquettes que vous pouvez définir et attribuer à certains types de AWS ressources, notamment aux objets S3. Chaque balise se compose d'une clé de balise obligatoire et d'une valeur de balise facultative. Pour plus d'informations sur le balisage des objets S3, consultez la section Catégorisation de votre stockage à l'aide de balises dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Pour une tâche de découverte de données sensibles, vous pouvez utiliser ce type de condition pour inclure ou exclure des objets dotés d'une balise spécifique. Il peut s'agir d'une clé de balise spécifique ou d'une clé de balise et d'une valeur de balise spécifiques (par paire). Si vous spécifiez plusieurs balises comme valeurs pour une condition, Macie utilise la logique OR pour joindre les valeurs. Par exemple, si vous spécifiez **`Project1`** et **`Project2`** en tant que clés de balise pour une condition, tout objet doté de la clé de balise Project1 ou Project2 répond aux critères de la condition.

Notez que les clés et les valeurs des balises distinguent les majuscules et minuscules. De plus, Macie ne prend pas en charge l'utilisation de valeurs partielles ou de caractères génériques dans ce type de condition.

Création d'une tâche de découverte de données sensibles

Avec Amazon Macie, vous pouvez créer et exécuter des tâches de découverte de données sensibles afin d'automatiser la découverte, la journalisation et le reporting des données sensibles dans les compartiments à usage général Amazon Simple Storage Service (Amazon S3). Une tâche de découverte de données sensibles est une série de tâches de traitement et d'analyse automatisées que Macie exécute pour détecter et signaler les données sensibles dans les objets Amazon S3. Au fur et à mesure que l'analyse progresse, Macie fournit des rapports détaillés sur les données sensibles qu'elle trouve et sur l'analyse qu'elle effectue : les résultats de données sensibles, qui signalent les données sensibles trouvées par Macie dans des objets S3 individuels, et les résultats de découverte de données sensibles, qui enregistrent les détails de l'analyse des objets S3 individuels. Pour plus d'informations, consultez Examiner les statistiques et les résultats des emplois.

Lorsque vous créez une tâche, vous commencez par spécifier les compartiments S3 qui contiennent les objets que vous souhaitez que Macie analyse lors de l'exécution de la tâche, qu'il s'agisse de compartiments spécifiques que vous sélectionnez ou de compartiments répondant à des critères spécifiques. Vous spécifiez ensuite la fréquence d'exécution de la tâche : une fois ou périodiquement sur une base quotidienne, hebdomadaire ou mensuelle. Vous pouvez également choisir des options pour affiner la portée de l'analyse de la tâche. Les options incluent des critères personnalisés qui découlent des propriétés des objets S3, telles que les balises, les préfixes et la date de dernière modification d'un objet.

Après avoir défini le calendrier et l'étendue de la tâche, vous spécifiez les identifiants de données gérés et les identifiants de données personnalisés à utiliser :

- Un identifiant de données géré est un ensemble de critères et de techniques intégrés conçus pour détecter un type spécifique de données sensibles, par exemple les numéros de carte de crédit, les clés d'accès AWS secrètes ou les numéros de passeport d'un pays ou d'une région en particulier. Ces identifiants peuvent détecter une liste longue et croissante de types de données sensibles pour de nombreux pays et régions, notamment plusieurs types de données d'identification, d'informations financières et d'informations personnelles identifiables (PII). Pour plus d'informations, consultez Utilisation des identificateurs de données gérés.
- Un identificateur de données personnalisé est un ensemble de critères que vous définissez pour détecter les données sensibles. Grâce aux identifiants de données personnalisés, vous pouvez détecter les données sensibles qui reflètent les scénarios particuliers de votre entreprise, la propriété intellectuelle ou les données propriétaires, par exemple les identifiants des employés, les numéros de compte client ou les classifications de données internes. Vous pouvez compléter les identifiants de données gérés fournis par Macie. Pour plus d'informations, consultez Création d'identificateurs de données personnalisés.

Vous pouvez ensuite éventuellement sélectionner Autoriser l'utilisation des listes. Une liste d'autorisation indique le texte ou un modèle de texte que vous souhaitez que Macie ignore, généralement des exceptions relatives aux données sensibles pour vos scénarios ou votre environnement particuliers, par exemple les noms publics ou les numéros de téléphone de votre organisation, ou des exemples de données que votre organisation utilise pour les tests. Pour plus d'informations, consultez Définition des exceptions relatives aux données sensibles à l'aide de listes d'autorisation.

Lorsque vous avez fini de choisir ces options, vous êtes prêt à saisir les paramètres généraux de la tâche, tels que le nom et la description de la tâche. Vous pouvez ensuite consulter et enregistrer le travail.

Tâches

Avant de commencer

Avant de créer une tâche, il est conseillé de suivre les étapes suivantes :

- Vérifiez que vous avez configuré un référentiel pour les résultats de la découverte de vos données sensibles. Pour ce faire, choisissez Discovery results dans le volet de navigation de la console Amazon Macie. Pour en savoir plus sur ces paramètres, consultezStockage et conservation des résultats de découverte de données sensibles.
- Créez les identificateurs de données personnalisés que vous souhaitez que la tâche utilise. Pour savoir comment procéder, veuillez consulter la section Création d'identificateurs de données personnalisés.
- Créez les listes d'autorisation que vous souhaitez que la tâche utilise. Pour savoir comment procéder, veuillez consulter la section Création et gestion de listes d'autorisations.
- Si vous souhaitez analyser des objets S3 chiffrés, assurez-vous que Macie peut accéder aux clés de chiffrement appropriées et les utiliser. Pour plus d'informations, consultez Analyse des objets S3 chiffrés.
- Si vous souhaitez analyser des objets dans un compartiment S3 soumis à une politique de compartiment restrictive, assurez-vous que Macie est autorisé à accéder aux objets. Pour plus d'informations, consultez Autoriser Macie à accéder aux compartiments et aux objets S3.

Si vous effectuez ces opérations avant de créer une tâche, vous rationalisez la création de la tâche et vous contribuez à ce que la tâche puisse analyser les données souhaitées.

Étape 1 : Choisissez des compartiments S3

Lorsque vous créez une tâche, la première étape consiste à spécifier quels compartiments S3 stockent les objets que vous souhaitez que Macie analyse lors de l'exécution de la tâche. Pour cette étape, deux options s'offrent à vous :

- Sélectionnez des compartiments spécifiques : avec cette option, vous sélectionnez explicitement chaque compartiment S3 à analyser. Ensuite, lorsque la tâche s'exécute, elle analyse les objets uniquement dans les compartiments que vous sélectionnez.
- Spécifier les critères de compartiment : avec cette option, vous définissez des critères d'exécution qui déterminent les compartiments S3 à analyser. Les critères se composent d'une ou de plusieurs conditions dérivées des propriétés du compartiment. Ensuite, lorsque la tâche s'exécute, elle identifie les compartiments correspondant à vos critères et analyse les objets qu'ils contiennent.

Pour des informations détaillées sur ces options, consultez Options d'étendue pour les tâches.

Les sections suivantes fournissent des instructions pour choisir et configurer chaque option. Choisissez la section correspondant à l'option souhaitée.

Sélectionnez des seaux spécifiques

Si vous choisissez de sélectionner explicitement chaque compartiment S3 à analyser, Macie vous fournit un inventaire complet de vos compartiments à usage général actuels. Région AWS Vous pouvez ensuite utiliser cet inventaire pour sélectionner un ou plusieurs compartiments pour la tâche. Pour en savoir plus sur cet inventaire, consultezSélection de compartiments S3 spécifiques.

Si vous êtes l'administrateur Macie d'une organisation, l'inventaire inclut les buckets détenus par les comptes des membres de votre organisation. Vous pouvez sélectionner jusqu'à 1 000 de ces compartiments, couvrant jusqu'à 1 000 comptes.

Pour sélectionner des compartiments S3 spécifiques pour la tâche

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, sélectionnez Tâches.
3. Choisissez Créer une tâche.

4. Sur la page Choisir des compartiments S3, choisissez Sélectionner des compartiments spécifiques. Macie affiche un tableau de tous les compartiments à usage général pour votre compte dans la région actuelle.
5. Dans la section Select S3 buckets, choisissez éventuellement refresh
()
pour récupérer les dernières métadonnées de bucket depuis Amazon S3.

   Si l'icône d'information
()
apparaît à côté d'un nom de bucket, nous vous recommandons de le faire. Cette icône indique qu'un bucket a été créé au cours des dernières 24 heures, probablement après que Macie ait récupéré pour la dernière fois les métadonnées du bucket et de l'objet sur Amazon S3 dans le cadre du cycle d'actualisation quotidien.
6. Dans le tableau, cochez la case correspondant à chaque compartiment que vous souhaitez que la tâche analyse.

> **Tip**
>
> - Pour trouver plus facilement des compartiments spécifiques, entrez les critères de filtre dans la zone de filtre située au-dessus du tableau. Vous pouvez également trier le tableau en choisissant un titre de colonne.
> - Pour déterminer si vous avez déjà configuré une tâche pour analyser régulièrement les objets d'un compartiment, reportez-vous au champ Surveillé par tâche. Si Oui apparaît dans un champ, le compartiment est explicitement inclus dans une tâche périodique ou le compartiment a répondu aux critères d'une tâche périodique au cours des dernières 24 heures. En outre, le statut d'au moins un de ces emplois n'est pas annulé. Macie met à jour ces données quotidiennement.
> - Pour déterminer à quel moment une tâche périodique ou ponctuelle existante a analysé le plus récemment des objets d'un bucket, reportez-vous au champ Dernière exécution de la tâche. Pour plus d'informations sur cette tâche, reportez-vous aux détails du bucket.
> - Pour afficher les détails d'un bucket, choisissez le nom du bucket. Outre les informations relatives au travail, le panneau de détails fournit des statistiques et d'autres informations sur le bucket, telles que les paramètres d'accès public du bucket.

Pour en savoir plus sur ces données, consultezRévision de l'inventaire de votre compartiment S3.

7. Lorsque vous avez fini de sélectionner les compartiments, choisissez Next.

À l'étape suivante, vous allez revoir et vérifier vos sélections.

Spécifier les critères du compartiment

Si vous choisissez de spécifier des critères d'exécution qui déterminent les compartiments S3 à analyser, Macie propose des options pour vous aider à choisir les champs, les opérateurs et les valeurs correspondant aux conditions individuelles dans les critères. Pour en savoir plus sur ces options, consultez Spécification des critères du compartiment S3.

Pour spécifier les critères du compartiment S3 pour la tâche

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, sélectionnez Tâches.
3. Choisissez Créer une tâche.
4. Sur la page Choisir des compartiments S3, choisissez Spécifier les critères du compartiment.
5. Sous Spécifier les critères du compartiment, procédez comme suit pour ajouter une condition aux critères :

    a. Placez votre curseur dans la zone de filtre, puis choisissez la propriété bucket à utiliser pour la condition.

    b. Dans la première case, choisissez un opérateur pour la condition, égal ou non égal.

    c. Dans la zone suivante, entrez une ou plusieurs valeurs pour la propriété.

    Selon le type et la nature de la propriété du bucket, Macie propose différentes options pour saisir des valeurs. Par exemple, si vous choisissez la propriété Autorisation effective, Macie affiche une liste de valeurs parmi lesquelles choisir. Si vous choisissez la propriété Account ID, Macie affiche une zone de texte dans laquelle vous pouvez saisir un ou plusieurs Compte AWS identifiants. Pour saisir plusieurs valeurs dans une zone de texte, entrez chaque valeur et séparez chaque entrée par une virgule.

    d. Choisissez Appliquer. Macie ajoute la condition et l'affiche sous la boîte de filtre.

Par défaut, Macie ajoute la condition avec une instruction include. Cela signifie que la tâche est configurée pour analyser (inclure) des objets dans des compartiments qui répondent à la condition. Pour ignorer (exclure) les compartiments correspondant à la condition, choisissez Inclure pour la condition, puis choisissez Exclure.

e. Répétez les étapes précédentes pour chaque condition supplémentaire que vous souhaitez ajouter aux critères.

6. Pour tester vos critères, élargissez la section Aperçu des résultats des critères. Cette section affiche un tableau des compartiments à usage général qui répondent actuellement aux critères.
7. Pour affiner vos critères, effectuez l'une des opérations suivantes :

   - Pour supprimer une condition, choisissez X comme condition.
   - Pour modifier une condition, supprimez-la en choisissant X comme condition. Ajoutez ensuite une condition dont les paramètres sont corrects.
   - Pour supprimer toutes les conditions, choisissez Effacer les filtres.

   Macie met à jour le tableau des résultats des critères pour refléter vos modifications.
8. Lorsque vous avez fini de définir les critères du compartiment, choisissez Next.

À l'étape suivante, vous allez revoir et vérifier vos critères.

Étape 2 : passez en revue vos sélections ou critères de compartiment S3

Pour cette étape, vérifiez que vous avez choisi les bons paramètres à l'étape précédente :

- Passez en revue vos sélections de compartiments - Si vous avez sélectionné des compartiments S3 spécifiques pour la tâche, consultez le tableau des compartiments et modifiez vos sélections de compartiments si nécessaire. Le tableau donne un aperçu de la portée et du coût prévus de l'analyse du travail. Les données sont basées sur la taille et le type des objets actuellement stockés dans un bucket.

  Dans le tableau, le champ Coût estimé indique le coût total estimé (en dollars américains) de l'analyse des objets dans un compartiment S3. Chaque estimation reflète la quantité prévue de données non compressées que la tâche analysera dans un bucket. Si des objets sont compressés ou des fichiers d'archive, l'estimation suppose que les fichiers utilisent un taux de compression de 3:1 et que la tâche peut analyser tous les fichiers extraits. Pour plus d'informations, consultez Prévision et surveillance des coûts des travaux.

- Passez en revue les critères de votre compartiment - Si vous avez spécifié des critères de compartiment pour le travail, passez en revue chaque condition des critères. Pour modifier les critères, choisissez Précédent, puis utilisez les options de filtre de l'étape précédente pour saisir les bons critères. Lorsque vous avez terminé, choisissez Suivant.

Lorsque vous avez terminé de vérifier et de vérifier les paramètres, choisissez Next.

Étape 3 : définir le calendrier et affiner le périmètre

Pour cette étape, spécifiez la fréquence à laquelle vous souhaitez que la tâche soit exécutée : une fois ou périodiquement sur une base quotidienne, hebdomadaire ou mensuelle. Choisissez également différentes options pour affiner la portée de l'analyse de la tâche. Pour en savoir plus sur ces options, consultezOptions d'étendue pour les tâches.

Pour définir le calendrier et affiner l'étendue du travail

1. Sur la page Affiner le champ d'application, spécifiez la fréquence à laquelle vous souhaitez que le travail soit exécuté :

   - Pour exécuter la tâche une seule fois, immédiatement après l'avoir créée, choisissez Tâche unique.
   - Pour exécuter la tâche de façon périodique et récurrente, choisissez la tâche planifiée. Pour la fréquence des mises à jour, choisissez si vous souhaitez exécuter la tâche quotidiennement, chaque semaine ou chaque mois. Utilisez ensuite l'option Inclure les objets existants pour définir l'étendue de la première exécution de la tâche :
     - Cochez cette case pour analyser tous les objets existants immédiatement après avoir créé la tâche. Chaque exécution suivante analyse uniquement les objets créés ou modifiés après l'exécution précédente.
     - Décochez cette case pour ignorer l'analyse de tous les objets existants. La première exécution de la tâche analyse uniquement les objets créés ou modifiés une fois que vous avez terminé de créer la tâche et avant le début de la première exécution. Chaque exécution suivante analyse uniquement les objets créés ou modifiés après l'exécution précédente.

       La désactivation de cette case à cocher est utile lorsque vous avez déjà analysé les données et que vous souhaitez continuer à les analyser régulièrement. Par exemple, si vous avez déjà utilisé un autre service ou une autre application pour classer les données et que vous avez récemment commencé à utiliser Macie, vous pouvez utiliser cette option pour

garantir la découverte et la classification continues de vos données sans encourir de coûts inutiles ni dupliquer les données de classification.

2. (Facultatif) Pour spécifier le pourcentage d'objets que vous souhaitez que la tâche analyse, entrez le pourcentage dans le champ Profondeur d'échantillonnage.

   Si cette valeur est inférieure à 100 %, Macie sélectionne les objets à analyser au hasard, jusqu'au pourcentage spécifié, et analyse toutes les données contenues dans ces objets. La valeur par défaut est 100 %.

3. (Facultatif) Pour ajouter des critères spécifiques qui déterminent quels objets S3 sont inclus ou exclus de l'analyse de la tâche, développez la section Paramètres supplémentaires, puis entrez les critères. Ces critères consistent en des conditions individuelles qui découlent des propriétés des objets :

   - Pour analyser (inclure) des objets répondant à une condition spécifique, entrez le type et la valeur de la condition, puis choisissez Inclure.
   - Pour ignorer (exclure) les objets qui répondent à une condition spécifique, entrez le type et la valeur de la condition, puis choisissez Exclure.

   Répétez cette étape pour chaque condition d'inclusion ou d'exclusion que vous souhaitez.

   Si vous entrez plusieurs conditions, les conditions d'exclusion ont priorité sur les conditions d'inclusion. Par exemple, si vous incluez des objets portant l'extension de nom de fichier .pdf et que vous excluez des objets dont la taille est supérieure à 5 Mo, la tâche analyse tout objet portant l'extension de nom de fichier .pdf, sauf si l'objet est supérieur à 5 Mo.

4. Lorsque vous avez terminé, choisissez Suivant.

Étape 4 : Sélectionnez les identifiants de données gérés

Pour cette étape, spécifiez les identifiants de données gérés que vous souhaitez que la tâche utilise lorsqu'elle analyse des objets S3. Vous avez deux options :

- Utiliser les paramètres recommandés - Avec cette option, la tâche analyse les objets S3 à l'aide de l'ensemble d'identifiants de données gérés que nous recommandons pour les tâches. Cet ensemble est conçu pour détecter les catégories et types courants de données sensibles. Pour consulter la liste des identificateurs de données gérés figurant actuellement dans l'ensemble, consultezIdentificateurs de données gérés recommandés pour les tâches. Nous mettons à jour

cette liste chaque fois que nous ajoutons ou supprimons un identifiant de données gérées dans l'ensemble.

- Utiliser des paramètres personnalisés - Avec cette option, la tâche analyse les objets S3 à l'aide d'identifiants de données gérés que vous sélectionnez. Il peut s'agir de la totalité ou de certains des identifiants de données gérés actuellement disponibles. Vous pouvez également configurer la tâche pour qu'elle n'utilise aucun identifiant de données géré. La tâche peut à la place utiliser uniquement les identifiants de données personnalisés que vous sélectionnez à l'étape suivante. Pour consulter la liste des identificateurs de données gérés actuellement disponibles, consultezRéférence rapide : identifiants de données gérés par Amazon Macie. Nous mettons à jour cette liste chaque fois que nous publions un nouvel identifiant de données gérées.

Lorsque vous choisissez l'une ou l'autre option, Macie affiche un tableau des identificateurs de données gérées. Dans le tableau, le champ Type de données sensibles indique l'identifiant unique (ID) d'un identifiant de données gérées. Cet identifiant décrit le type de données sensibles que l'identifiant de données gérées est conçu pour détecter, par exemple : USA_PASSPORT_NUMBER pour les numéros de passeport américains, CREDIT_CARD_NUMBER pour les numéros de carte de crédit et PGP_PRIVATE_KEY pour les clés privées PGP. Pour trouver des identifiants spécifiques plus rapidement, vous pouvez trier et filtrer le tableau par catégorie ou type de données sensibles.

Pour sélectionner des identifiants de données gérés pour la tâche

1. Sur la page Sélectionner les identifiants de données gérés, sous Options d'identifiant de données gérées, effectuez l'une des opérations suivantes :

   - Pour utiliser l'ensemble d'identifiants de données gérés que nous recommandons pour les tâches, choisissez Recommandé.

     Si vous choisissez cette option et que vous avez configuré le travail pour qu'il soit exécuté plusieurs fois, chaque exécution utilise automatiquement tous les identificateurs de données gérés figurant dans l'ensemble recommandé au début de l'exécution. Cela inclut les nouveaux identifiants de données gérés que nous publions et ajoutons à l'ensemble. Cela exclut les identifiants de données gérés que nous supprimons de l'ensemble et que nous ne recommandons plus pour les tâches.

   - Pour utiliser uniquement les identificateurs de données gérées spécifiques que vous sélectionnez, choisissez Personnalisé, puis choisissez Utiliser des identifiants de données gérées spécifiques. Dans le tableau, cochez ensuite la case correspondant à chaque identifiant de données gérées que vous souhaitez que la tâche utilise.

Si vous choisissez cette option et que vous avez configuré le travail pour qu'il s'exécute plusieurs fois, chaque exécution utilise uniquement les identificateurs de données gérés que vous sélectionnez. En d'autres termes, la tâche utilise ces mêmes identifiants de données gérées à chaque fois qu'elle s'exécute.

- Pour utiliser tous les identifiants de données gérés actuellement fournis par Macie, choisissez Personnalisé, puis choisissez Utiliser des identifiants de données gérées spécifiques. Dans le tableau, cochez ensuite la case dans l'en-tête de la colonne de sélection pour sélectionner toutes les lignes.

  Si vous choisissez cette option et que vous avez configuré le travail pour qu'il s'exécute plusieurs fois, chaque exécution utilise uniquement les identificateurs de données gérés que vous sélectionnez. En d'autres termes, la tâche utilise ces mêmes identifiants de données gérées à chaque fois qu'elle s'exécute.
- Pour ne pas utiliser d'identifiants de données gérés et n'utiliser que des identifiants de données personnalisés, choisissez Personnalisé, puis choisissez Ne pas utiliser d'identifiants de données gérées. Ensuite, à l'étape suivante, sélectionnez les identifiants de données personnalisés à utiliser.

2. Lorsque vous avez terminé, choisissez Suivant.

Étape 5 : Sélectionnez des identifiants de données personnalisés

Pour cette étape, sélectionnez les identifiants de données personnalisés que vous souhaitez que la tâche utilise lorsqu'elle analyse des objets S3. La tâche utilisera les identifiants sélectionnés en plus des identifiants de données gérées pour lesquels vous avez configuré la tâche. Pour en savoir plus sur les identificateurs de données personnalisés, consultezCréation d'identificateurs de données personnalisés.

Pour sélectionner des identifiants de données personnalisés pour la tâche

1. Sur la page Sélectionner des identifiants de données personnalisés, cochez la case correspondant à chaque identifiant de données personnalisé que vous souhaitez que la tâche utilise. Vous pouvez sélectionner jusqu'à 30 identifiants de données personnalisés.

   > **Tip**
   >
   > Pour vérifier ou tester les paramètres d'un identifiant de données personnalisé avant de le sélectionner, cliquez sur l'icône de lien

()
à côté du nom de l'identifiant. Macie ouvre une page qui affiche les paramètres de l'identifiant.
Vous pouvez également utiliser cette page pour tester l'identifiant à l'aide d'échantillons de données. Pour ce faire, entrez jusqu'à 1 000 caractères de texte dans la zone Exemple de données, puis choisissez Test. Macie évalue l'échantillon de données à l'aide de l'identifiant, puis indique le nombre de correspondances.

2. Lorsque vous avez fini de sélectionner des identificateurs de données personnalisés, choisissez Next.

Étape 6 : Sélectionnez les listes autorisées

Pour cette étape, sélectionnez les listes d'autorisation que vous souhaitez que la tâche utilise lorsqu'elle analyse des objets S3. Pour en savoir plus sur les listes d'autorisation, voirDéfinition des exceptions relatives aux données sensibles à l'aide de listes d'autorisation.

Pour sélectionner des listes d'autorisation pour le travail

1. Sur la page Sélectionner les listes d'autorisation, cochez la case correspondant à chaque liste d'autorisation que vous souhaitez que le travail utilise. Vous pouvez sélectionner jusqu'à 10 listes.

> **Tip**
>
> Pour vérifier les paramètres d'une liste d'autorisation avant de la sélectionner, cliquez sur l'icône de lien
> ()
> à côté du nom de la liste. Macie ouvre une page qui affiche les paramètres de la liste. Si la liste indique une expression régulière (regex), vous pouvez également utiliser cette page pour tester l'expression régulière avec des exemples de données. Pour ce faire, entrez jusqu'à 1 000 caractères de texte dans la zone Exemple de données, puis choisissez Test. Macie évalue les exemples de données à l'aide de l'expression régulière, puis indique le nombre de correspondances.

2. Lorsque vous avez fini de sélectionner les listes autorisées, choisissez Next.

Étape 7 : Entrez les paramètres généraux

Pour cette étape, spécifiez un nom et, éventuellement, une description de la tâche. Vous pouvez également attribuer des balises à la tâche. Un tag est un label que vous définissez et attribuez à certains types de AWS ressources. Chaque balise comprend une clé de balise obligatoire et une valeur de balise facultative. Les balises peuvent vous aider à identifier, à classer et à gérer les ressources de différentes manières, par exemple en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Pour en savoir plus, veuillez consulter la section Marquage des ressources Amazon Macie.

Pour saisir les paramètres généraux de la tâche

1. Sur la page Entrer les paramètres généraux, entrez le nom de la tâche dans le champ Nom de la tâche. Le nom peut contenir jusqu'à 500 caractères.
2. (Facultatif) Dans le champ Description du poste, entrez une brève description du poste. La description peut contenir jusqu'à 200 caractères.
3. (Facultatif) Pour les balises, choisissez Ajouter une étiquette, puis entrez jusqu'à 50 balises à attribuer à la tâche.
4. Lorsque vous avez terminé, choisissez Suivant.

Étape 8 : Réviser et créer

Pour cette dernière étape, passez en revue les paramètres de configuration de la tâche et vérifiez qu'ils sont corrects. C'est une étape importante. Une fois que vous avez créé une tâche, vous ne pouvez modifier aucun de ces paramètres. Cela permet de garantir que vous disposez d'un historique immuable des découvertes relatives aux données sensibles et des résultats de découverte pour les audits ou enquêtes que vous effectuez sur la confidentialité et la protection des données.

En fonction des paramètres de la tâche, vous pouvez également consulter le coût total estimé (en dollars américains) de l'exécution unique de la tâche. Si vous avez sélectionné des compartiments S3 spécifiques pour la tâche, l'estimation est basée sur la taille et le type d'objets contenus dans les compartiments sélectionnés, ainsi que sur la quantité de données que la tâche peut analyser. Si vous avez défini des critères de compartiment pour la tâche, l'estimation est basée sur la taille et le type d'objets contenus dans pas moins de 500 compartiments qui répondent actuellement aux critères, ainsi que sur la quantité de données que la tâche peut analyser. Pour en savoir plus sur cette estimation, voirPrévision et surveillance des coûts des travaux.

Pour consulter et créer le poste

1. Sur la page Réviser et créer, passez en revue chaque paramètre et vérifiez qu'il est correct. Pour modifier un paramètre, choisissez Modifier dans la section contenant le paramètre, puis entrez le paramètre correct. Vous pouvez également utiliser les onglets de navigation pour accéder à la page contenant un paramètre.
2. Lorsque vous avez terminé de vérifier les paramètres, choisissez Soumettre pour créer et enregistrer le travail. Macie vérifie les paramètres et vous informe de tout problème à résoudre.

   > **Note**
   >
   > Si vous n'avez pas configuré de référentiel pour vos résultats de découverte de données sensibles, Macie affiche un avertissement et n'enregistre pas le travail. Pour résoudre ce problème, choisissez Configurer dans la section Référentiel pour les résultats de découverte de données sensibles. Entrez ensuite les paramètres de configuration du référentiel. Pour savoir comment procéder, veuillez consulter la section Stockage et conservation des résultats de découverte de données sensibles. Après avoir saisi les paramètres, revenez à la page Réviser et créer, puis sélectionnez Actualiser () dans la section Référentiel pour les résultats de découverte de données sensibles de la page.
   >
   > Bien que cela ne soit pas recommandé, vous pouvez temporairement annuler les exigences du référentiel et enregistrer le travail. Si vous le faites, vous risquez de perdre les résultats de la recherche : Macie ne les conservera que pendant 90 jours. Pour annuler temporairement cette exigence, cochez la case correspondant à l'option de dérogation.

3. Si Macie vous signale des problèmes à résoudre, résolvez-les, puis cliquez à nouveau sur Soumettre pour créer et enregistrer le travail.

Si vous avez configuré le travail pour qu'il s'exécute une fois, tous les jours ou le jour de la semaine ou du mois en cours, Macie commence à exécuter le travail immédiatement après l'avoir enregistré. Sinon, Macie se prépare à exécuter la tâche le jour de la semaine ou du mois spécifié. Pour surveiller la tâche, vous pouvez vérifier le statut de la tâche.

Examen des statistiques et des résultats pour les tâches de découverte de données sensibles

Lorsque vous exécutez une tâche de découverte de données sensibles, Amazon Macie calcule et rapporte automatiquement certaines données statistiques pour la tâche. Par exemple, Macie indique le nombre de fois que la tâche a été exécutée et le nombre approximatif d'objets Amazon Simple Storage Service (Amazon S3) que la tâche n'a pas encore traités au cours de son exécution en cours. Macie produit également plusieurs types de résultats pour cette tâche : événements de journalisation, résultats de découverte de données sensibles et résultats de découverte de données sensibles.

Rubriques

Types de résultats pour les tâches de découverte de données sensibles

Au fur et à mesure qu'une tâche de découverte de données sensibles progresse, Amazon Macie produit les types de résultats suivants pour cette tâche.

Enregistrer un événement

Il s'agit d'un enregistrement d'un événement qui s'est produit pendant l'exécution de la tâche. Macie enregistre et publie automatiquement les données de certains événements sur Amazon CloudWatch Logs. Les données de ces journaux fournissent un enregistrement des modifications apportées à la progression ou à l'état de la tâche, telles que la date et l'heure exactes auxquelles la tâche a commencé ou s'est arrêtée. Les données fournissent également des détails sur les erreurs de compte ou de compartiment survenues pendant l'exécution de la tâche.

Les événements du journal peuvent vous aider à surveiller une tâche et à résoudre les problèmes qui empêchaient la tâche d'analyser les données souhaitées. Si une tâche utilise des critères d'exécution pour déterminer les compartiments S3 à analyser, les événements du journal peuvent également vous aider à déterminer si et quels compartiments S3 répondaient aux critères lors de l'exécution de la tâche.

Vous pouvez accéder aux événements du journal à l'aide de la CloudWatch console Amazon ou de l'API Amazon CloudWatch Logs. Pour vous aider à accéder aux événements du journal d'une

tâche, la console Amazon Macie fournit un lien vers ces événements. Pour plus d'informations, consultez Surveillance de tâche .

Recherche de données sensibles

Il s'agit d'un rapport concernant des données sensibles que Macie a trouvées dans un objet S3. Chaque résultat fournit une note de gravité et des détails tels que :

- Date et heure auxquelles Macie a trouvé les données sensibles.
- Catégorie et types de données sensibles détectées par Macie.
- Le nombre d'occurrences de chaque type de données sensibles détectées par Macie.
- Identifiant unique de la tâche à l'origine de la recherche.
- Le nom, les paramètres d'accès public, le type de chiffrement et les autres informations relatives au compartiment et à l'objet S3 concernés.

Selon le type de fichier ou le format de stockage de l'objet S3 concerné, les détails peuvent également inclure l'emplacement de 15 occurrences des données sensibles détectées par Macie. Pour signaler les données de localisation, les résultats de données sensibles utilisent un schéma JSON standardisé.

Une découverte de données sensibles n'inclut pas les données sensibles trouvées par Macie. Il fournit plutôt des informations que vous pouvez utiliser pour des recherches plus approfondies et des mesures correctives si nécessaire.

Macie conserve les résultats de données sensibles pendant 90 jours. Vous pouvez y accéder à l'aide de la console Amazon Macie ou de l'API Amazon Macie. Vous pouvez également les surveiller et les traiter à l'aide d'autres applications, services et systèmes. Pour plus d'informations, consultez Analyse des résultats.

Résultat de la découverte de données sensibles

Il s'agit d'un enregistrement qui enregistre les détails relatifs à l'analyse d'un objet S3. Macie crée automatiquement un résultat de découverte de données sensibles pour chaque objet que vous configurez une tâche à analyser. Cela inclut les objets dans lesquels Macie ne trouve aucune donnée sensible et ne produit donc pas de données sensibles, ainsi que les objets que Macie ne peut pas analyser en raison d'erreurs ou de problèmes tels que les paramètres d'autorisation ou l'utilisation d'un format de fichier ou de stockage non pris en charge.

Si Macie trouve des données sensibles dans un objet S3, le résultat de la découverte de données sensibles inclut les données issues de la recherche de données sensibles correspondante. Il

fournit également des informations supplémentaires, telles que l'emplacement de pas moins de 1 000 occurrences de chaque type de données sensibles trouvées par Macie dans l'objet. Par exemple :

- Numéro de colonne et de ligne d'une cellule ou d'un champ dans un classeur Microsoft Excel, un fichier CSV ou un fichier TSV
- Le chemin d'accès à un champ ou à un tableau dans un fichier JSON ou JSON Lines
- Numéro de ligne d'une ligne dans un fichier texte non binaire autre qu'un fichier CSV, JSON, JSON Lines ou TSV, par exemple un fichier HTML, TXT ou XML
- Numéro de page d'une page dans un fichier Adobe Portable Document Format (PDF)
- L'index d'enregistrement et le chemin d'accès à un champ dans un enregistrement d'un conteneur d'objets Apache Avro ou d'un fichier Apache Parquet

Si l'objet S3 concerné est un fichier d'archive, tel qu'un fichier .tar ou .zip, le résultat de la découverte de données sensibles fournit également des données de localisation détaillées pour les occurrences de données sensibles dans des fichiers individuels que Macie a extraits de l'archive. Macie n'inclut pas ces informations dans les résultats de données sensibles pour les fichiers d'archive. Pour signaler les données de localisation, les résultats de découverte de données sensibles utilisent un schéma JSON standardisé.

Un résultat de découverte de données sensibles n'inclut pas les données sensibles trouvées par Macie. Il vous fournit plutôt un enregistrement d'analyse qui peut être utile pour les audits ou enquêtes sur la confidentialité et la protection des données.

Macie conserve les résultats de la découverte de vos données sensibles pendant 90 jours. Vous ne pouvez pas y accéder directement depuis la console Amazon Macie ou via l'API Amazon Macie. Au lieu de cela, vous configurez Macie pour les chiffrer et les stocker dans un compartiment S3. Le bucket peut servir de référentiel définitif à long terme pour tous vos résultats de découverte de données sensibles. Vous pouvez ensuite éventuellement accéder aux résultats de ce référentiel et les interroger. Pour savoir comment configurer ces paramètres, consultezStockage et conservation des résultats de découverte de données sensibles.

Après avoir configuré les paramètres, Macie écrit les résultats de la découverte de vos données sensibles dans des fichiers JSON Lines (.jsonl), puis chiffre et ajoute ces fichiers au compartiment S3 sous forme de fichiers GNU Zip (.gz). Pour vous aider à accéder aux résultats, la console Amazon Macie fournit des liens vers ces derniers.

Les découvertes de données sensibles et les résultats de découverte de données sensibles respectent tous deux des schémas standardisés. Cela peut éventuellement vous aider à les interroger, à les surveiller et à les traiter à l'aide d'autres applications, services et systèmes.

> **Tip**
>
> Pour un exemple détaillé et instructif de la manière dont vous pouvez interroger et utiliser les résultats de découverte de données sensibles pour analyser et signaler les risques potentiels liés à la sécurité des données, consultez le billet de blog Comment interroger et visualiser les résultats de découverte de données sensibles de Macie avec Amazon Athena et QuickSight Amazon AWS sur le blog de sécurité.
> Pour obtenir des exemples de requêtes Amazon Athena que vous pouvez utiliser pour analyser les résultats de découverte de données sensibles, consultez le référentiel Amazon Macie Results Analytics sur. GitHub Ce référentiel fournit également des instructions pour configurer Athena afin de récupérer et de déchiffrer vos résultats, ainsi que des scripts pour créer des tables pour les résultats.

Révision des statistiques et des résultats pour une tâche de découverte de données sensibles

Pour consulter les statistiques de traitement et les résultats des différentes tâches de découverte de données sensibles, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie. Suivez ces étapes pour consulter les statistiques et les résultats d'une tâche à l'aide de la console.

Pour accéder aux statistiques de traitement d'une tâche par programmation, utilisez l'DescribeClassificationJobAPI Amazon Macie. Pour accéder par programmation aux résultats produits par une tâche, utilisez le ListFindingsfonctionnement de l'API Amazon Macie et spécifiez l'identifiant unique de la tâche dans une condition de filtre pour `classificationDetails.jobId` le champ. Pour savoir comment procéder, veuillez consulter la section Création et application de filtres aux résultats. Vous pouvez ensuite utiliser l'GetFindingsopération pour récupérer les détails des résultats.

Pour consulter les statistiques et les résultats d'une offre d'emploi

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, sélectionnez Tâches.

3. Sur la page Tâches, choisissez le nom de la tâche dont vous souhaitez consulter les statistiques et les résultats. Le panneau de détails affiche les statistiques, les paramètres et d'autres informations relatives à la tâche.
4. Dans le panneau de détails, effectuez l'une des opérations suivantes :

   - Pour consulter les statistiques de traitement de la tâche, reportez-vous à la section Statistiques du panneau. Cette section affiche des statistiques telles que le nombre de fois que le travail a été exécuté et le nombre approximatif d'objets que le travail n'a pas encore traités au cours de son exécution en cours.
   - Pour consulter les événements du journal de la tâche, choisissez Afficher les résultats en haut du panneau, puis Afficher CloudWatch les journaux. Macie ouvre la CloudWatch console Amazon et affiche un tableau des événements du journal publiés par Macie pour la tâche.
   - Pour consulter tous les résultats relatifs aux données sensibles produits par le travail, choisissez Afficher les résultats en haut du panneau, puis choisissez Afficher les résultats. Macie ouvre la page Résultats et affiche tous les résultats de la tâche. Pour consulter les détails d'un résultat en particulier, choisissez le résultat, puis reportez-vous au panneau des détails.

     > **Tip**
     >
     > Dans le panneau des détails de la recherche, vous pouvez utiliser le lien dans le champ Emplacement détaillé des résultats pour accéder au résultat de découverte de données sensibles correspondant dans Amazon S3 :
     >
     > - Si le résultat s'applique à une archive volumineuse ou à un fichier compressé, le lien affiche le dossier contenant les résultats de la découverte du fichier. Une archive ou un fichier compressé est volumineux s'il génère plus de 100 résultats de découverte.
     > - Si le résultat s'applique à une petite archive ou à un fichier compressé, le lien affiche le fichier contenant les résultats de la découverte du fichier. Une archive ou un fichier compressé est petit s'il génère 100 résultats de découverte ou moins.
     > - Si le résultat s'applique à un autre type de fichier, le lien affiche le fichier contenant les résultats de la découverte du fichier.

   - Pour consulter tous les résultats de découverte de données sensibles produits par le travail, choisissez Afficher les résultats en haut du panneau, puis Afficher les classifications. Macie ouvre la console Amazon S3 et affiche le dossier contenant tous les résultats de découverte

de la tâche. Cette option n'est disponible qu'après avoir configuré Macie pour stocker les résultats de la découverte de données sensibles dans un compartiment S3.

Surveillance des tâches de découverte de données sensibles avec Amazon CloudWatch Logs

Outre le suivi de l'état général d'une tâche de découverte de données sensibles, vous pouvez surveiller et analyser des événements spécifiques qui se produisent au fur et à mesure de l'avancement d'une tâche. Vous pouvez le faire en utilisant des données de journalisation en temps quasi réel qu'Amazon Macie publie automatiquement sur Amazon CloudWatch Logs. Les données de ces journaux fournissent un enregistrement des modifications apportées à la progression ou à l'état d'une tâche, telles que la date et l'heure exactes auxquelles une tâche a commencé à s'exécuter, a été suspendue ou s'est terminée.

Les données du journal fournissent également des détails sur les erreurs de compte ou de compartiment survenant lors de l'exécution d'une tâche. Par exemple, si les paramètres d'autorisation d'un compartiment S3 empêchent une tâche d'analyser les objets du compartiment, Macie enregistre un événement. L'événement indique à quel moment l'erreur s'est produite et identifie à la fois le bucket concerné et le compte propriétaire du bucket. Les données relatives à ces types d'événements peuvent vous aider à identifier, à étudier et à corriger les erreurs qui empêchent Macie d'analyser les données souhaitées.

Avec Amazon CloudWatch Logs, vous pouvez surveiller, stocker et accéder aux fichiers journaux provenant de plusieurs systèmes, applicationsServices AWS, y compris Macie. Vous pouvez également interroger et analyser les données des journaux, et configurer les CloudWatch journaux pour qu'ils vous avertissent lorsque certains événements se produisent ou que des seuils sont atteints. CloudWatch Logs fournit également des fonctionnalités permettant d'archiver les données des journaux et de les exporter vers Amazon S3. Pour en savoir plus sur CloudWatch les journaux, consultez le guide de l'utilisateur Amazon CloudWatch Logs.

Rubriques

- Comment fonctionne la journalisation pour les tâches de découverte de données sensibles
- Examen des journaux pour les tâches de découverte de données sensibles
- Schéma des événements de journal pour les tâches de découverte de données sensibles
- Types d'événements de journalisation pour les tâches de découverte de données sensibles

Comment fonctionne la journalisation pour les tâches de découverte de données sensibles

Lorsque vous commencez à exécuter des tâches de découverte de données sensibles, Macie crée et configure automatiquement les ressources appropriées dans Amazon CloudWatch Logs pour enregistrer les événements relatifs à toutes vos tâches en cours. Région AWS Macie publie ensuite automatiquement les données des événements sur ces ressources lorsque vos tâches sont exécutées. La politique d'autorisation pour le rôle lié au service Macie pour votre compte permet à Macie d'effectuer ces tâches en votre nom. Vous n'avez pas besoin de prendre de mesures pour créer ou configurer des ressources dans CloudWatch Logs, ni pour enregistrer les données d'événements pour vos tâches.

Dans CloudWatch Logs, les logs sont organisés en groupes de logs. Chaque groupe de journaux contient des flux de journaux. Chaque flux de journal contient des événements de journal. L'objectif général de chacune de ces ressources est le suivant :

- Un groupe de journaux est un ensemble de flux de journaux qui partagent les mêmes paramètres de conservation, de surveillance et de contrôle d'accès, par exemple la collecte de journaux pour toutes vos tâches de découverte de données sensibles.
- Un flux de journal est une séquence d'événements de journal qui partagent la même source, par exemple une tâche individuelle de découverte de données sensibles.
- Un événement de journal est un enregistrement d'une activité enregistrée par une application ou une ressource, par exemple un événement individuel enregistré et publié par Macie pour une tâche de découverte de données sensibles particulière.

Macie publie les événements de toutes vos tâches de découverte de données sensibles dans un seul groupe de journaux, et chaque tâche possède un flux de journal unique dans ce groupe de journaux. Le groupe de journaux porte le préfixe et le nom suivants :

```
/aws/macie/classificationjobs
```

Si ce groupe de journaux existe déjà, Macie l'utilise pour stocker les événements liés à vos tâches. Cela peut être utile si votre organisation utilise une configuration automatisée, par exemple pour créer des groupes de journaux avec des périodes de conservation des journaux prédéfinies, des paramètres de chiffrement, des balises, des filtres métriques, etc. pour les événements professionnels. AWS CloudFormation

Si ce groupe de journaux n'existe pas, Macie le crée avec les paramètres par défaut utilisés par Logs pour les nouveaux groupes de CloudWatch journaux. Les paramètres incluent une période de conservation des journaux Never Expire, ce qui signifie que CloudWatch Logs stocke les journaux indéfiniment. Pour modifier la période de conservation du groupe de journaux, vous pouvez utiliser la CloudWatch console Amazon ou l'API Amazon CloudWatch Logs. Pour savoir comment procéder, consultez la section Utilisation des groupes de journaux et des flux de CloudWatch journaux dans le guide de l'utilisateur Amazon Logs.

Au sein de ce groupe de journaux, Macie crée un flux de journal unique pour chaque tâche que vous exécutez, la première fois que la tâche est exécutée. Le nom du flux de journal est l'identifiant unique de la tâche, par exemple `85a55dc0fa6ed0be5939d0408example` dans le format suivant.

```
/aws/macie/classificationjobs/85a55dc0fa6ed0be5939d0408example
```

Chaque flux de journal contient tous les événements de journal que Macie a enregistrés et publiés pour la tâche correspondante. Pour les tâches périodiques, cela inclut les événements relatifs à toutes les exécutions de la tâche. Si vous supprimez le flux de journal pour une tâche périodique, Macie le crée à nouveau lors de la prochaine exécution de la tâche. Si vous supprimez le flux de journal pour une tâche ponctuelle, vous ne pouvez pas le restaurer.

Notez que la journalisation est activée par défaut pour toutes vos tâches. Vous ne pouvez pas le désactiver ou empêcher Macie de publier des événements professionnels dans CloudWatch Logs. Si vous ne souhaitez pas stocker les journaux, vous pouvez réduire la période de conservation du groupe de journaux à un jour seulement. À la fin de la période de conservation, CloudWatch Logs supprime automatiquement les données d'événements expirées du groupe de journaux.

Examen des journaux pour les tâches de découverte de données sensibles

Vous pouvez consulter les journaux de vos tâches de découverte de données sensibles à l'aide de la CloudWatch console Amazon ou de l'API Amazon CloudWatch Logs. La console et l'API fournissent toutes deux des fonctionnalités conçues pour vous aider à consulter et à analyser les données du journal. Vous pouvez utiliser ces fonctionnalités pour gérer les flux de journaux et les événements liés à vos tâches, comme vous le feriez avec tout autre type de données de journal dans CloudWatch Logs.

Par exemple, vous pouvez rechercher et filtrer des données agrégées afin d'identifier des types spécifiques d'événements survenus pour toutes vos tâches au cours d'une période donnée. Vous pouvez également effectuer un examen ciblé de tous les événements survenus pour une tâche

donnée. CloudWatch Logs fournit également des options pour surveiller les données des journaux, définir des filtres métriques et créer des alarmes personnalisées.

> **Tip**
>
> Pour accéder aux événements du journal d'une tâche en particulier à l'aide de la console Amazon Macie, procédez comme suit : Sur la page Tâches, choisissez le nom de la tâche. En haut du panneau de détails, choisissez Afficher les résultats, puis Afficher CloudWatch les journaux. Macie ouvre la CloudWatch console Amazon et affiche un tableau des événements du journal de la tâche.

Pour consulter les journaux de vos tâches (CloudWatch console Amazon)

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous avez exécuté les tâches dont vous souhaitez consulter les journaux.
3. Dans le panneau de navigation de gauche, choisissez Logs (Journaux), puis Log groups (Groupes de journaux).
4. Sur la page Groupes de journaux, choisissez le groupe de journaux /aws/macie/classificationjobs. CloudWatch Logs affiche un tableau des flux de journaux pour les tâches que vous avez exécutées. Il existe un flux unique pour chaque tâche. Le nom de chaque flux correspond à l'identifiant unique d'une tâche.
5. Sous Log streams, effectuez l'une des opérations suivantes :

   - Pour consulter les événements du journal d'une tâche en particulier, choisissez le flux de journal correspondant à la tâche. Pour trouver le flux plus facilement, entrez l'identifiant unique de la tâche dans le champ de filtre situé au-dessus du tableau. Une fois que vous avez choisi le flux de journal, CloudWatch Logs affiche un tableau des événements de journal relatifs à la tâche.
   - Pour consulter les événements du journal de toutes vos tâches, choisissez Rechercher dans tous les flux de journaux. CloudWatch Logs affiche un tableau des événements du journal pour toutes vos tâches.
6. (Facultatif) Dans la zone de filtre située au-dessus du tableau, entrez des termes, des phrases ou des valeurs qui spécifient les caractéristiques des événements spécifiques à examiner. Pour plus d'informations, consultez la section Rechercher dans les données des journaux à l'aide de modèles de filtre dans le guide de l'utilisateur Amazon CloudWatch Logs.

7. Pour consulter les détails d'un événement de journal spécifique, cliquez sur la flèche droite (▶) dans la ligne correspondant à l'événement. CloudWatch Logs affiche les détails de l'événement au format JSON.

Au fur et à mesure que vous vous familiarisez avec les données des événements du journal, vous pouvez également effectuer des tâches telles que la création de filtres de mesures qui transforment les données du journal en CloudWatch mesures numériques, et la création d'alarmes personnalisées qui vous permettent d'identifier et de répondre plus facilement à des événements de journal spécifiques. Pour plus d'informations, consultez le guide de l'utilisateur Amazon CloudWatch Logs.

Schéma des événements de journal pour les tâches de découverte de données sensibles

Chaque événement de journal pour une tâche de découverte de données sensibles est un objet JSON conforme au schéma d'événements Amazon CloudWatch Logs et contenant un ensemble standard de champs. Certains types d'événements comportent des champs supplémentaires qui fournissent des informations particulièrement utiles pour ce type d'événement. Par exemple, les événements liés à des erreurs au niveau du compte incluent l'ID de compte de la personne concernée. Compte AWS Les événements liés à des erreurs au niveau du compartiment incluent le nom du compartiment S3 concerné. Pour une liste détaillée des événements professionnels publiés par Macie sur CloudWatch Logs, consultezTypes d'événements de journalisation pour les offres d'emploi.

L'exemple suivant montre le schéma des événements du journal pour les tâches de découverte de données sensibles. Dans cet exemple, l'événement indique que Macie n'a pu analyser aucun objet dans un compartiment S3 car Amazon S3 a refusé l'accès au compartiment.

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "BUCKET_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:11:30.574809Z",
    "description": "Macie doesn't have permission to access the affected S3 bucket.",
    "jobName": "My_Macie_Job",
    "operation": "ListObjectsV2",
    "runDate": "2021-04-14T17:08:30.345809Z",
    "affectedAccount": "111122223333",
    "affectedResource": {
```

```
        "type": "S3_BUCKET_NAME",
        "value": "DOC-EXAMPLE-BUCKET"
    }
}
```

Dans l'exemple précédent, Macie a tenté de répertorier les objets du compartiment en utilisant l'opération ListObjectsV2 de l'API Amazon S3. Lorsque Macie a envoyé la demande à Amazon S3, Amazon S3 a refusé l'accès au compartiment.

Les champs suivants sont communs à tous les événements de journalisation relatifs aux tâches de découverte de données sensibles :

- `adminAccountId`— L'identifiant unique de la personne Compte AWS qui a créé la tâche.
- `jobId`— L'identifiant unique de la tâche.
- `eventType`— Le type d'événement qui s'est produit. Pour obtenir la liste complète des valeurs possibles et une description de chacune d'entre elles, voirTypes d'événements de journalisation pour les offres d'emploi.
- `occurredAt`— La date et l'heure, en temps universel coordonné (UTC) et au format ISO 8601 étendu, auxquelles l'événement s'est produit.
- `description`— Une brève description de l'événement.
- `jobName`— Le nom personnalisé de la tâche.

Selon le type et la nature d'un événement, un événement de journal peut également contenir les champs suivants :

- `affectedAccount`— L'identifiant unique du propriétaire Compte AWS de la ressource affectée.
- `affectedResource`— Un objet qui fournit des informations sur la ressource affectée. Dans l'objet, le `type` champ indique un champ qui stocke les métadonnées relatives à une ressource. Le `value` champ indique la valeur du champ (`type`).
- `operation`— L'opération que Macie a tenté d'effectuer et qui est à l'origine de l'erreur.
- `runDate`— Date et heure, en temps universel coordonné (UTC) et au format ISO 8601 étendu, du début de la tâche ou de l'exécution de la tâche applicable.

Types d'événements de journalisation pour les tâches de découverte de données sensibles

Macie publie des événements de journal pour trois catégories d'événements :

- Événements relatifs au statut d'une tâche, qui enregistrent les modifications apportées au statut ou à la progression d'une tâche ou d'une exécution de tâche.
- Événements d'erreur au niveau du compte, qui enregistrent les erreurs qui ont empêché Macie d'analyser les données Amazon S3 pour une recherche spécifique. Compte AWS
- Événements d'erreur au niveau du compartiment, qui enregistrent les erreurs qui ont empêché Macie d'analyser les données d'un compartiment S3 spécifique.

Les rubriques de cette section répertorient et décrivent les types d'événements publiés par Macie pour chaque catégorie.

Rubriques

Événements relatifs au statut des emplois

Un événement relatif au statut d'une tâche enregistre une modification du statut ou de la progression d'une tâche ou d'une exécution de tâche. Pour les tâches périodiques, Macie enregistre et publie ces événements à la fois pour l'ensemble de la tâche et pour l'exécution des tâches individuelles. Pour plus d'informations sur la détermination du statut général d'une tâche, consultezVérification de l'état des tâches de découverte de données sensibles.

L'exemple suivant utilise des exemples de données pour montrer la structure et la nature des champs lors d'un événement relatif au statut d'une tâche. Dans cet exemple, un `SCHEDULED_RUN_COMPLETED` événement indique que l'exécution planifiée d'une tâche périodique s'est terminée. La course a débuté le 14 avril 2021 à 17:09:30 UTC, comme indiqué sur le `runDate` terrain. La course s'est terminée le 14 avril 2021 à 17 h 16 h 30 UTC, comme indiqué sur le `occurredAt` terrain.

```
{
    "adminAccountId": "123456789012",
```

```
    "jobId": "ffad0e71455f38a4c7c220f3cexample",
    "eventType": "SCHEDULED_RUN_COMPLETED",
    "occurredAt": "2021-04-14T17:16:30.574809Z",
    "description": "The scheduled job run finished running.",
    "jobName": "My_Daily_Macie_Job",
    "runDate": "2021-04-14T17:09:30.574809Z"
}
```

Le tableau suivant répertorie et décrit les types d'événements relatifs à l'état des tâches que Macie enregistre et publie dans CloudWatch Logs. La colonne Type d'événement indique le nom de chaque événement tel qu'il apparaît dans le `eventType` champ d'un événement. La colonne Description fournit une brève description de l'événement tel qu'il apparaît dans le `description` champ d'un événement. Les informations supplémentaires fournissent des informations sur le type de tâche auquel s'applique l'événement. Le tableau est d'abord trié selon l'ordre chronologique général dans lequel les événements peuvent se produire, puis par ordre alphabétique croissant par type d'événement.

Type d'événement	Description	Informations supplémentaires
EMPLOI CRÉÉ	L'emploi a été créé.	S'applique aux tâches ponctuelles et périodiques.
UN SEUL TRAVAIL A COMMENCÉ	La tâche a commencé à s'exécuter.	S'applique uniquement aux tâches ponctuelles.
SCHEDULED_RUN_STARTED	L'exécution de la tâche planifiée a commencé à s'exécuter.	S'applique uniquement aux tâches périodiques. Pour enregistrer le début d'une tâche ponctuelle, Macie publie un événement ONE_TIME_JOB_STARTED, pas ce type d'événement.
LE SEAU CORRESPONDAIT AUX CRITÈRES	Le compartiment concerné correspondait aux critères de	S'applique aux tâches ponctuelles et périodiques qui utilisent les critères des

Type d'événement	Description	Informations supplémentaires
	compartiment spécifiés pour la tâche.	compartiments d'exécution pour déterminer les compartiments S3 à analyser. L'`affectedResource` objet indique le nom du compartiment qui correspond aux critères et qui a été inclus dans l'analyse de la tâche.
AUCUN SEAU NE CORRESPONDAIT AUX CRITÈRES	La tâche a commencé à s'exécuter mais aucun compartiment ne correspond actuellement aux critères de compartiment spécifiés pour la tâche. Le travail n'a analysé aucune donnée.	S'applique aux tâches ponctuelles et périodiques qui utilisent les critères des compartiments d'exécution pour déterminer les compartiments S3 à analyser.
SCHEDULED_RUN_COMPLETED	L'exécution de la tâche planifiée s'est terminée.	S'applique uniquement aux tâches périodiques. Pour enregistrer l'achèvement d'une tâche ponctuelle, Macie publie un événement JOB_COMPLETED, et non ce type d'événement.
JOB_PAUSED_BY_USER	La tâche a été interrompue par un utilisateur.	S'applique aux tâches ponctuelles et périodiques que vous avez arrêtées temporairement (suspendues).

Type d'événement	Description	Informations supplémentaires
REPRISE DU TRAVAIL PAR L'UTILISATEUR	La tâche a été reprise par un utilisateur.	S'applique aux tâches ponctuelles et périodiques que vous avez arrêtées temporairement (suspendues) puis reprises.
JOB_PAUSED_BY_MACIE_SERVICE_QUOTA_MET	Le travail a été suspendu par Macie. L'achèvement du travail dépasserait le quota mensuel pour le compte concerné.	S'applique aux tâches ponctuelles et périodiques que Macie a temporairement arrêtées (suspendues). Macie suspend automatiquement une tâche lorsque le traitement supplémentaire effectué par la tâche ou l'exécution d'une tâche dépasse le quota mensuel de découverte de données sensibles pour un ou plusieurs comptes pour lesquels la tâche analyse les données. Pour éviter ce problème, pensez à augmenter le quota des comptes concernés.

Type d'événement	Description	Informations supplémentaires
JOB_RESUMED_BY_MACIE_SERVICE_QUOTA_LIFTED	Le travail a été repris par Macie. Le quota de service mensuel a été levé pour le compte concerné.	S'applique aux tâches ponctuelles et périodiques que Macie a arrêtées temporairement (mises en pause) puis reprises. Si Macie a automatiquement suspendu une tâche ponctuelle, Macie reprend automatiquement la tâche au début du mois suivant ou le quota mensuel de découverte de données sensibles est augmenté pour tous les comptes concernés, selon la première éventualité. Si Macie a automatiquement suspendu une tâche périodique, Macie reprend automatiquement la tâche au début de la prochaine exécution ou au début du mois suivant, selon la première éventualité.

Type d'événement	Description	Informations supplémentaires
JOB ANNULÉ	Le travail a été annulé.	S'applique aux tâches ponctuelles et périodiqu es que vous avez arrêtées définitivement (annulées) ou, pour les tâches ponctuell es, suspendues et que vous n'avez pas reprises dans les 30 jours. Si vous suspendez ou désactivez Macie, ce type d'événement s'applique également aux tâches qui étaient actives ou suspendue s lorsque vous avez suspendu ou désactivé Macie. Macie annule automatiquement vos tâches Région AWS si vous suspendez ou désactivez Macie dans la région.
TÂCHE TERMINÉE	L'exécution de la tâche s'est terminée.	S'applique uniquement aux tâches ponctuelles. Pour enregistrer la fin d'une tâche exécutée pour une tâche périodique, Macie publie un événement SCHEDULED _RUN_COMPLETED, pas ce type d'événement.

Événements d'erreur au niveau du compte

Un événement d'erreur au niveau du compte enregistre une erreur qui a empêché Macie d'analyser des objets dans des compartiments S3 appartenant à une personne spécifique. Compte AWS Le `affectedAccount` champ de chaque événement indique l'ID de compte de ce compte.

L'exemple suivant utilise des exemples de données pour montrer la structure et la nature des champs lors d'un événement d'erreur au niveau du compte. Dans cet exemple, un `ACCOUNT_ACCESS_DENIED` événement indique que Macie n'a pas été en mesure d'analyser les objets dans les compartiments S3 appartenant à un compte. `444455556666`

```
{
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "ACCOUNT_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:08:30.585709Z",
    "description": "Macie doesn't have permission to access S3 bucket data for the
 affected account.",
    "jobName": "My_Macie_Job",
    "operation": "ListBuckets",
    "runDate": "2021-04-14T17:05:27.574809Z",
    "affectedAccount": "444455556666"
}
```

Le tableau suivant répertorie et décrit les types d'événements d'erreur au niveau du compte que Macie enregistre et publie dans Logs. CloudWatch La colonne Type d'événement indique le nom de chaque événement tel qu'il apparaît dans le `eventType` champ d'un événement. La colonne Description fournit une brève description de l'événement tel qu'il apparaît dans le `description` champ d'un événement. La colonne Informations supplémentaires fournit tous les conseils applicables pour rechercher ou corriger l'erreur survenue. Le tableau est trié par ordre alphabétique croissant par type d'événement.

Type d'événement	Description	Informations supplémentaires
ACCESS_DE_COMPTE_REFUSÉ	Macie n'est pas autorisé à accéder aux données du compartiment S3 pour le compte concerné.	Cela se produit généralement parce que les compartiments détenus par le compte sont soumis à des politiques de compartiment restricti

Type d'événement	Description	Informations supplémentaires
		ves. Pour plus d'informations sur la manière de résoudre ce problème, consultez Autoriser Macie à accéder aux compartiments et aux objets S3. La valeur du `operation` champ de l'événement peut vous aider à déterminer quels paramètres d'autorisation ont empêché Macie d'accéder aux données S3 du compte. Ce champ indique l'opération Amazon S3 que Macie a tenté d'effectuer lorsque l'erreur s'est produite.
COMPTE_DÉSACTIVÉ	La tâche ignorait les ressources détenues par le compte concerné. Macie a été désactivée pour le compte.	Pour résoudre ce problème, réactivez Macie pour le compte dans celui-ci. Région AWS

Type d'événement	Description	Informations supplémentaires
COMPTE_DISSOCIÉ	La tâche ignorait les ressources détenues par le compte concerné. Le compte n'est plus associé à votre compte administrateur Macie en tant que compte membre.	Cela se produit si, en tant qu'administrateur Macie d'une organisation, vous configurez une tâche pour analyser les données d'un compte de membre associé et que le compte de membre est ensuite supprimé de votre organisation. Pour résoudre ce problème, associez à nouveau le compte concerné à votre compte administrateur Macie en tant que compte membre. Pour plus d'informations, veuillez consulter Gestion de plusieurs comptes .
COMPTE_ISOLÉ	La tâche ignorait les ressources détenues par le compte concerné. Ils Compte AWS étaient isolés.	–
COMPTE_RÉGION_DÉSACTIVÉ	La tâche ignorait les ressources détenues par le compte concerné. Le Compte AWS n'est pas actif en ce momentRégion AWS.	–

Type d'événement	Description	Informations supplémentaires
COMPTE_SUSPENDU	La tâche a été annulée ou des ressources appartena nt au compte concerné ont été ignorées. Macie a été suspendu pour ce compte.	Si le compte indiqué est le vôtre, Macie a automatiq uement annulé le travail lorsque vous avez suspendu Macie dans la même région. Pour résoudre ce problème, réactivez Macie dans la région. Si le compte spécifié est un compte membre, réactivez Macie pour ce compte dans la même région.
COMPTE RÉSILIÉ	La tâche ignorait les ressource s détenues par le compte concerné. Compte AWSIl a été résilié.	–

Événements d'erreur au niveau du bucket

Un événement d'erreur au niveau du compartiment enregistre une erreur qui a empêché Macie d'analyser des objets dans un compartiment S3 spécifique. Le `affectedAccount` champ de chaque événement indique l'ID de compte du Compte AWS propriétaire du bucket. Dans chaque événement, l'`affectedResource`objet indique le nom du compartiment.

L'exemple suivant utilise des exemples de données pour montrer la structure et la nature des champs lors d'un événement d'erreur au niveau du compartiment. Dans cet exemple, un `BUCKET_ACCESS_DENIED` événement indique que Macie n'a pu analyser aucun objet dans le compartiment S3 nommé`DOC-EXAMPLE-BUCKET`. Lorsque Macie a tenté de répertorier les objets du compartiment en utilisant l'opération ListObjectsV2 de l'API Amazon S3, Amazon S3 a refusé l'accès au compartiment.

```
{
```

```
    "adminAccountId": "123456789012",
    "jobId": "85a55dc0fa6ed0be5939d0408example",
    "eventType": "BUCKET_ACCESS_DENIED",
    "occurredAt": "2021-04-14T17:11:30.574809Z",
    "description": "Macie doesn't have permission to access the affected S3 bucket.",
    "jobName": "My_Macie_Job",
    "operation": "ListObjectsV2",
    "runDate": "2021-04-14T17:09:30.685209Z",
    "affectedAccount": "111122223333",
    "affectedResource": {
        "type": "S3_BUCKET_NAME",
        "value": "DOC-EXAMPLE-BUCKET"
    }
}
```

Le tableau suivant répertorie et décrit les types d'événements d'erreur au niveau du compartiment que Macie enregistre et publie dans Logs. CloudWatch La colonne Type d'événement indique le nom de chaque événement tel qu'il apparaît dans le `eventType` champ d'un événement. La colonne Description fournit une brève description de l'événement tel qu'il apparaît dans le `description` champ d'un événement. La colonne Informations supplémentaires fournit tous les conseils applicables pour rechercher ou corriger l'erreur survenue. Le tableau est trié par ordre alphabétique croissant par type d'événement.

Type d'événement	Description	Informations supplémentaires
BUCKET_ACCESS_DENIED	Macie n'est pas autorisé à accéder au compartiment S3 concerné.	Cela se produit généralement parce qu'un compartiment est soumis à une politique de compartiment restrictive. Pour plus d'informations sur la manière de résoudre ce problème, consultez Autoriser Macie à accéder aux compartiments et aux objets S3. La valeur du `operation` champ de l'événement peut vous aider à déterminer quels

Type d'événement	Description	Informations supplémentaires
		paramètres d'autorisation ont empêché Macie d'accéder au bucket. Ce champ indique l'opération Amazon S3 que Macie a tenté d'effectuer lorsque l'erreur s'est produite.
DÉTAILS DU GODET NON DISPONIBLES	Un problème temporaire a empêché Macie de récupérer des informations sur le compartiment et ses objets.	Cela se produit si un problème temporaire a empêché Macie de récupérer les métadonné es du bucket et de l'objet dont il a besoin pour analyser les objets d'un bucket. Par exemple, une exception Amazon S3 s'est produite lorsque Macie a essayé de vérifier qu'elle était autorisée à accéder au compartiment. Pour résoudre le problème lié à une tâche ponctuell e, envisagez de créer et d'exécuter une nouvelle tâche ponctuelle pour analyser les objets du compartiment. Pour une tâche planifiée, Macie essaiera à nouveau de récupérer les métadonnées lors de la prochaine exécution de la tâche.
LE GODET N'EXISTE PAS	Le compartiment S3 concerné n'existe plus.	Cela se produit généralement parce qu'un compartiment a été supprimé.

Type d'événement	Description	Informations supplémentaires
SEAU DANS UNE RÉGION DIFFÉRENTE	Le compartiment S3 concerné a été déplacé vers un autreRégion AWS.	–
LE PROPRIÉTAIRE DU GODET A CHANGÉ	Le propriétaire du compartiment S3 concerné a changé. Macie n'est plus autorisé à accéder au bucket.	Cela se produit généralement si la propriété d'un bucket a été transférée à un Compte AWS utilisateur ne faisant pas partie de votre organisation. Le `affectedAccount` champ de l'événement indique l'ID de compte du compte qui possédait auparavant le bucket.

Gestion des tâches de découverte de données sensibles

Pour vous aider à gérer vos tâches de découverte de données sensibles, Amazon Macie fournit un inventaire complet de vos tâches dans chacune d'elles. Région AWS Grâce à cet inventaire, vous pouvez gérer vos tâches en tant que collection unique et accéder aux paramètres de configuration, au statut et aux statistiques de traitement des tâches individuelles. Vous pouvez également accéder aux données sensibles et aux autres résultats produits par chaque tâche.

Outre ces tâches, vous pouvez créer des variantes personnalisées de tâches individuelles : copier une tâche existante, ajuster les paramètres de la copie, puis enregistrer la copie en tant que nouvelle tâche. Cela peut être utile dans les cas où vous souhaitez analyser différents ensembles de données de la même manière, ou le même ensemble de données de différentes manières. Vous souhaitez également ajuster les paramètres de configuration d'une tâche existante : annulez la tâche existante, copiez-la, puis ajustez et enregistrez la copie en tant que nouvelle tâche.

Rubriques

- Révision de votre inventaire des tâches de découverte de données sensibles
- Révision des paramètres de configuration pour les tâches de découverte de données sensibles

- Vérification de l'état des tâches de découverte de données sensibles
- Suspension, reprise ou annulation de tâches de découverte de données sensibles
- Copier des tâches de découverte de données sensibles

Révision de votre inventaire des tâches de découverte de données sensibles

La page Jobs de la console Amazon Macie fournit des informations sur toutes les tâches de découverte de données sensibles actuellement associées à votre compte. Région AWS Pour chaque tâche, le tableau affiche des informations récapitulatives qui incluent : le statut actuel de la tâche ; si la tâche s'exécute de manière planifiée et périodique ; et si la tâche analyse un nombre spécifique de compartiments S3 ou si elle analyse des compartiments S3 qui répondent aux critères d'exécution. Si vous choisissez une tâche dans le tableau, le panneau de détails affiche les paramètres de configuration et d'autres informations relatives à la tâche.

Pour consulter votre inventaire des emplois

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, sélectionnez Tâches. La page Tâches s'ouvre et affiche le nombre de tâches figurant dans votre inventaire ainsi qu'un tableau de ces tâches.
3. Pour trouver un emploi spécifique plus rapidement, effectuez l'une des opérations suivantes :

   - Pour trier le tableau en fonction d'un champ spécifique, choisissez l'en-tête de colonne du champ. Pour modifier l'ordre de tri, choisissez à nouveau l'en-tête de colonne.
   - Pour afficher uniquement les tâches qui ont une valeur spécifique pour un champ, placez votre curseur dans la zone de filtre. Dans le menu qui apparaît, choisissez le champ à utiliser pour le filtre, puis entrez la valeur du filtre. Choisissez ensuite Apply(Applisuer).
   - Pour masquer les tâches qui ont une valeur spécifique pour un champ, placez votre curseur dans la zone de filtre. Dans le menu qui apparaît, choisissez le champ à utiliser pour le filtre, puis entrez la valeur du filtre. Choisissez ensuite Apply(Applisuer). Dans la zone de filtre, choisissez l'icône égale (●) pour le filtre. Cela fait passer l'opérateur du filtre de égal à non égal (⌀).
   - Pour supprimer un filtre, cliquez sur l'icône de suppression du filtre (⊗) correspondant au filtre à supprimer.

4. Pour consulter les paramètres de configuration et d'autres informations relatives à une tâche particulière, choisissez le nom de la tâche dans le tableau, puis reportez-vous au panneau de détails.

Révision des paramètres de configuration pour les tâches de découverte de données sensibles

Sur la console Amazon Macie, vous pouvez utiliser le panneau de détails de la page Tâches pour consulter les paramètres de configuration et d'autres informations relatives aux tâches de découverte de données sensibles individuelles. Par exemple, vous pouvez consulter la liste des compartiments S3 qu'une tâche est configurée pour analyser et les identifiants de données gérés qu'une tâche utilise pour analyser les objets de ces compartiments.

> **Note**
>
> Vous ne pouvez modifier aucun paramètre de configuration pour une tâche existante. Cela permet de garantir que vous disposez d'un historique immuable des découvertes relatives aux données sensibles et des résultats de découverte pour les audits ou enquêtes que vous effectuez sur la confidentialité et la protection des données. Si vous souhaitez modifier une tâche existante, annulez-la. Copiez ensuite la tâche, configurez la copie pour utiliser les paramètres souhaités et enregistrez la copie en tant que nouvelle tâche.
> Dans ce cas, vous devez également prendre des mesures pour vous assurer que la nouvelle tâche n'analyse pas à nouveau les données existantes de la même manière. Pour ce faire, notez la date et l'heure auxquelles vous annulez le travail existant. Configurez ensuite l'étendue de la nouvelle tâche pour inclure uniquement les objets créés ou modifiés après l'annulation de la tâche d'origine. Par exemple, utilisez des critères d'objet pour ajouter une condition d'exclusion de dernière modification qui spécifie la date et l'heure auxquelles vous avez annulé le travail d'origine.

Pour consulter les paramètres de configuration d'une tâche

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, sélectionnez Tâches.
3. Sur la page Tâches, choisissez le nom de la tâche dont vous souhaitez vérifier les paramètres. Le panneau de détails affiche les paramètres de configuration et d'autres informations relatives à la tâche. En fonction des paramètres de la tâche, le panneau contient les sections suivantes.

Informations générales

Cette section fournit des informations générales sur la tâche, par exemple le nom de ressource Amazon (ARN) de la tâche, la date à laquelle la tâche a récemment commencé à s'exécuter et le statut actuel de la tâche. Si vous avez suspendu la tâche, cette section indique également à quel moment vous l'avez interrompue et à quel moment la tâche ou la dernière exécution de la tâche a expiré ou expirera si vous ne la reprenez pas.

Statistiques

Cette section présente les statistiques de traitement de la tâche, par exemple le nombre de fois que la tâche a été exécutée et le nombre approximatif d'objets que la tâche n'a pas encore traités pendant son exécution en cours.

Scope (Portée)

Cette section indique la fréquence d'exécution de la tâche. Il affiche également les paramètres qui affinent la portée de la tâche, par exemple la profondeur d'échantillonnage et tous les critères d'objet qui incluent ou excluent les objets S3 de l'analyse de la tâche.

Compartiments S3

Cette section apparaît dans le panneau si la tâche est configurée pour analyser les compartiments que vous avez explicitement sélectionnés lors de sa création. Il indique le numéro pour Comptes AWS lequel la tâche est configurée pour analyser les données. Il indique également le nombre de compartiments que la tâche est configurée pour analyser et les noms de ces compartiments (regroupés par compte).

Pour afficher la liste complète des comptes et des compartiments au format JSON, choisissez le numéro dans le champ Total des compartiments.

Critères du compartiment S3

Cette section apparaît dans le panneau si la tâche utilise des critères d'exécution pour déterminer les compartiments à analyser. Il répertorie les critères que la tâche est configurée pour utiliser.

Pour afficher les critères au format JSON, choisissez Détails, puis cliquez sur l'onglet Critères dans la fenêtre qui apparaît.

Pour consulter un tableau des compartiments qui répondent actuellement aux critères, cliquez sur Détails, puis sur l'onglet Compartiments correspondants dans la fenêtre qui apparaît. Choisissez éventuellement refresh () pour récupérer les dernières données.

> **Tip**
>
> Si la tâche a déjà été exécutée, vous pouvez également déterminer si des buckets répondaient aux critères lors de son exécution et, dans l'affirmative, les noms de ces buckets. Pour ce faire, passez en revue les événements du journal de la tâche : choisissez Afficher les résultats en haut du panneau, puis sélectionnez Afficher CloudWatch les journaux. Macie ouvre la CloudWatch console Amazon et affiche un tableau des événements du journal de la tâche. Les événements incluent un `BUCKET_MATCHED_THE_CRITERIA` événement pour chaque compartiment qui correspond aux critères et a été inclus dans l'analyse de la tâche. Pour plus d'informations, consultez Surveillance de tâche .

Identifiants de données personnalisés

Cette section apparaît dans le panneau si la tâche est configurée pour utiliser un ou plusieurs identifiants de données personnalisés. Il spécifie les noms de ces identifiants de données personnalisés.

Autoriser les listes

Cette section apparaît dans le panneau si la tâche est configurée pour utiliser une ou plusieurs listes d'autorisations. Il indique les noms de ces listes. Pour consulter les paramètres et le statut d'une liste, cliquez sur l'icône de lien () à côté du nom de la liste.

Identifiants de données gérés

Cette section indique les identifiants de données gérés pour lesquels la tâche est configurée. Ceci est déterminé par le type de sélection de l'identifiant de données géré pour la tâche :

- Recommandé : utilisez les identificateurs de données gérés figurant dans l'ensemble recommandé lors de l'exécution de la tâche.
- Inclure la sélection : utilisez uniquement les identifiants de données gérés répertoriés dans la section Sélections.
- Tout inclure : utilisez tous les identifiants de données gérés disponibles lors de l'exécution de la tâche.
- Exclure les données sélectionnées : utilisez tous les identifiants de données gérés disponibles lors de l'exécution de la tâche, à l'exception de ceux répertoriés dans la section Sélections.
- Tout exclure : n'utilisez aucun identifiant de données géré. Utilisez uniquement les identificateurs de données personnalisés spécifiés.

Pour consulter ces paramètres au format JSON, sélectionnez Détails.

Balises

Cette section apparaît dans le panneau si des balises sont associées à la tâche. Il répertorie ces tags.

Un tag est un label que vous définissez et attribuez à certains types de AWS ressources. Chaque balise comprend une clé de balise obligatoire et une valeur de balise facultative. Les balises peuvent vous aider à identifier, à classer et à gérer les ressources de différentes manières, par exemple en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Pour en savoir plus, veuillez consulter la section Marquage des ressources Amazon Macie.

4. Pour consulter et enregistrer les paramètres de la tâche au format JSON, choisissez l'identifiant unique de la tâche (Job ID) en haut du panneau, puis choisissez Download.

Vérification de l'état des tâches de découverte de données sensibles

Lorsque vous créez une tâche de découverte de données sensibles, son statut initial est Actif (Exécutif) ou Actif (Inactif), selon le type et le calendrier de la tâche. La tâche passe ensuite par d'autres états, que vous pouvez surveiller au fur et à mesure de son avancement.

> **Tip**
>
> Outre le suivi de l'état général d'une tâche, vous pouvez surveiller les événements spécifiques qui se produisent au fur et à mesure de l'avancement d'une tâche. Vous pouvez

le faire en utilisant les données de journalisation que Macie publie automatiquement sur Amazon CloudWatch Logs. Les données de ces journaux fournissent un enregistrement des modifications apportées au statut d'une tâche et des informations détaillées sur les erreurs de compte ou de compartiment survenant lors de l'exécution d'une tâche. Pour plus d'informations, consultez Surveillance de tâche .

Pour vérifier le statut d'une tâche

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, sélectionnez Tâches.
3. Sur la page Tâches, localisez la tâche dont vous souhaitez vérifier le statut. Le champ Status indique le statut actuel de la tâche.

   Actif (inactif)

   Pour une tâche périodique, l'exécution précédente est terminée et la prochaine exécution planifiée est en attente. Cette valeur ne s'applique pas aux tâches ponctuelles.

   Actif (course à pied)

   Pour une tâche ponctuelle, la tâche est actuellement en cours de réalisation. Pour une tâche périodique, une exécution planifiée est en cours.

   Annulée

   Quel que soit le type de tâche, la tâche a été définitivement arrêtée (annulée).

   Une tâche possède ce statut si vous l'avez explicitement annulée ou, s'il s'agit d'une tâche ponctuelle, si vous l'avez suspendue et ne l'avez pas reprise dans les 30 jours. Une offre d'emploi peut également avoir ce statut si vous avez suspendu Macie dans le passé. Région AWS

   Complet

   Pour une tâche ponctuelle, la tâche s'est exécutée correctement et est maintenant terminée. Cette valeur ne s'applique pas aux tâches périodiques. Au lieu de cela, le statut d'une tâche périodique passe à Active (Idle) lorsque chaque exécution est terminée avec succès.

En pause (par Macie)

Quel que soit le type de travail, le travail a été arrêté temporairement (suspendu) par Macie.

Une tâche possède ce statut si son achèvement ou son exécution dépassent le quota mensuel de découverte de données sensibles pour votre compte. Lorsque cela se produit, Macie met automatiquement le travail en pause. Macie reprend automatiquement le travail au début du mois civil suivant (et le quota mensuel est redéfini pour votre compte) ou lorsque vous augmentez le quota de votre compte.

Si vous êtes l'administrateur Macie d'une organisation et que vous avez configuré la tâche pour analyser les données des comptes des membres, la tâche peut également avoir ce statut si l'achèvement de la tâche ou l'exécution d'une tâche dépasse le quota mensuel de découverte de données sensibles pour un compte membre.

Si une tâche est en cours d'exécution et que l'analyse des objets éligibles atteint ce quota pour un compte membre, la tâche arrête d'analyser les objets appartenant au compte. Lorsque le travail a terminé d'analyser les objets pour tous les autres comptes n'ayant pas atteint le quota, Macie interrompt automatiquement le travail. S'il s'agit d'une tâche ponctuelle, Macie reprend automatiquement la tâche au début du mois civil suivant ou le quota est augmenté pour tous les comptes concernés, selon la première éventualité. S'il s'agit d'une tâche périodique, Macie reprend automatiquement la tâche au début de la prochaine exécution ou au début du mois civil suivant, selon la première éventualité. Si une exécution planifiée commence avant le début du mois civil suivant ou si le quota est augmenté pour un compte concerné, la tâche n'analyse pas les objets appartenant au compte.

En pause (par utilisateur)

Quel que soit le type de travail, vous l'avez arrêté temporairement (suspendu).

Si vous interrompez une tâche ponctuelle et que vous ne la reprenez pas dans les 30 jours, la tâche expire et Macie l'annule. Si vous interrompez une tâche périodique alors qu'elle est en cours d'exécution et que vous ne la reprenez pas dans les 30 jours, l'exécution de la tâche expire et Macie l'annule. Pour vérifier la date d'expiration d'une tâche suspendue ou d'une exécution de tâche, choisissez le nom de la tâche dans le tableau, puis reportez-vous au champ Expirations dans la section Détails du statut du panneau de détails.

Si une tâche est annulée ou suspendue, vous pouvez consulter les détails de la tâche pour déterminer si elle a commencé à s'exécuter ou, dans le cas d'une tâche périodique, si elle a été exécutée au moins une fois avant d'être annulée ou suspendue. Pour ce faire, choisissez le nom de la tâche dans le tableau, puis reportez-vous au panneau de détails. Dans le panneau, le champ Nombre d'exécutions indique le nombre de fois que la tâche a été exécutée. Le champ Date et heure de la dernière exécution indique la date et l'heure les plus récentes auxquelles le job a commencé à être exécuté.

En fonction de l'état actuel de la tâche, vous pouvez éventuellement la suspendre, la reprendre ou l'annuler.

Suspension, reprise ou annulation de tâches de découverte de données sensibles

Après avoir créé une tâche de découverte de données sensibles, vous pouvez la suspendre temporairement ou l'annuler définitivement. Lorsque vous suspendez une tâche en cours d'exécution, Macie commence immédiatement à suspendre toutes les tâches de traitement associées à cette tâche. Lorsque vous annulez une tâche en cours d'exécution, Macie commence immédiatement à arrêter toutes les tâches de traitement associées à cette tâche. Vous ne pouvez pas reprendre ou redémarrer une tâche une fois qu'elle a été annulée.

Si vous interrompez une tâche ponctuelle, vous pouvez la reprendre dans les 30 jours. Lorsque vous reprenez le travail, Macie reprend immédiatement le traitement à partir du point où vous l'avez suspendu. Macie ne le redémarre pas depuis le début. Si vous ne reprenez pas une tâche ponctuelle dans les 30 jours suivant son interruption, la tâche expire et Macie l'annule.

Si vous interrompez une tâche périodique, vous pouvez la reprendre à tout moment. Si vous reprenez une tâche périodique et que la tâche était inactive lorsque vous l'avez interrompue, Macie reprend la tâche conformément au calendrier et aux autres paramètres de configuration que vous avez choisis lors de la création de la tâche. Si vous reprenez une tâche périodique alors que la tâche était en cours d'exécution lorsque vous l'avez interrompue, la façon dont Macie reprend la tâche dépend de la date à laquelle vous reprenez la tâche :

- Si vous reprenez la tâche dans les 30 jours suivant son interruption, Macie reprend immédiatement la dernière exécution planifiée à partir du point où vous l'avez interrompue. Macie ne redémarre pas l'exécution depuis le début.
- Si vous ne reprenez pas le travail dans les 30 jours suivant son interruption, la dernière exécution planifiée expire et Macie annule toutes les tâches de traitement restantes pour l'exécution. Lorsque vous reprenez la tâche par la suite, Macie reprend la tâche conformément au calendrier et aux autres paramètres de configuration que vous avez choisis lors de la création de la tâche.

Pour vous aider à déterminer la date d'expiration d'une tâche suspendue ou d'une exécution de tâche, Macie ajoute une date d'expiration aux détails de la tâche pendant que celle-ci est suspendue. Pour vérifier cette date, choisissez le nom de la tâche dans le tableau de la page Tâches, puis reportez-vous au champ Expirations dans la section Détails du statut du panneau de détails. En outre, nous vous informons environ sept jours avant l'expiration de la tâche ou de l'exécution d'une tâche. Nous vous informons à nouveau lorsque la tâche ou l'exécution de la tâche expire et est annulée. Pour vous informer, nous envoyons un e-mail à l'adresse associée à votre Compte AWS. Nous créons également des AWS Health événements et Amazon CloudWatch Events pour votre compte.

Pour suspendre, reprendre ou annuler une tâche

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, sélectionnez Tâches.
3. Sur la page Tâches, cochez la case correspondant à la tâche que vous souhaitez suspendre, reprendre ou annuler, puis effectuez l'une des opérations suivantes dans le menu Actions :

   - Pour suspendre temporairement la tâche, choisissez Pause. Cette option n'est disponible que si le statut actuel de la tâche est Actif (Inactif), Actif (Exécution) ou Suspendu (Par Macie).
   - Pour reprendre le travail, choisissez Reprendre. Cette option n'est disponible que si le statut actuel de la tâche est Suspendu (par utilisateur).
   - Pour annuler définitivement le travail, choisissez Annuler. Si vous choisissez cette option, vous ne pourrez pas reprendre ou redémarrer le travail par la suite.

Copier des tâches de découverte de données sensibles

Pour créer rapidement une nouvelle tâche de découverte de données sensibles similaire à une tâche existante, vous pouvez créer une copie de la tâche, modifier les paramètres de la copie, puis enregistrer la copie en tant que nouvelle tâche. Cela peut être utile dans les cas où vous souhaitez créer une variante personnalisée d'une tâche existante. Vous souhaitez également ajuster les paramètres de configuration d'une tâche existante en annulant la tâche, puis en copiant, en modifiant et en enregistrant les paramètres en tant que nouvelle tâche.

Pour copier une tâche

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, sélectionnez Tâches.

3. Cochez la case correspondant à la tâche que vous souhaitez copier.
4. Dans le menu Actions, choisissez Copier vers un nouveau.
5. Effectuez les étapes sur la console pour vérifier et ajuster les paramètres de la copie de la tâche. Pour l'étape Affiner le champ d'application, pensez à choisir des options qui empêchent la tâche d'analyser à nouveau les données existantes de la même manière :

   - Pour une tâche ponctuelle, utilisez des critères d'objet pour n'inclure que les objets créés ou modifiés après un certain temps. Par exemple, si vous créez une copie d'un travail que vous avez annulé, ajoutez une condition Dernière modification qui précise la date et l'heure auxquelles vous avez annulé le travail existant.
   - Pour une tâche périodique, désactivez la case à cocher Inclure les objets existants. Dans ce cas, la première exécution de la tâche analyse uniquement les objets créés ou modifiés après la création de la tâche et avant la première exécution de la tâche. Vous pouvez également utiliser des critères d'objet pour exclure les objets qui ont été modifiés pour la dernière fois avant une certaine date et heure.

   Pour plus de détails à ce sujet et sur les autres étapes, consultezCréation d'une tâche de découverte de données sensibles.
6. Lorsque vous avez terminé, choisissez Soumettre pour enregistrer la copie en tant que nouvelle tâche.

Prédiction et surveillance des coûts pour les tâches de découverte de données sensibles

La tarification d'Amazon Macie est basée en partie sur la quantité de données que vous analysez en exécutant des tâches de découverte de données sensibles. Pour prévoir et surveiller les coûts estimés liés à l'exécution de tâches de découverte de données sensibles, vous pouvez consulter les estimations de coûts fournies par Macie lorsque vous créez une tâche et après avoir commencé à exécuter des tâches.

Pour vérifier et contrôler vos coûts réels, vous pouvez utiliserAWS Billing and Cost Management. AWS Billing and Cost Managementfournit des fonctionnalités conçues pour vous aider à suivre et à analyser vos coûts et à Services AWS gérer les budgets de votre compte ou de votre organisation. Il fournit également des fonctionnalités qui peuvent vous aider à prévoir les coûts d'utilisation sur la base de données historiques. Pour en savoir plus, consultez le AWS Billingguide de l'utilisateur.

Pour en savoir plus sur la tarification Macie, consultez la page sur la tarification d'Amazon Macie.

Rubriques

Prévision du coût d'une tâche de découverte de données sensibles

Lorsque vous créez une tâche de découverte de données sensibles, Amazon Macie peut calculer et afficher les coûts estimés au cours de deux étapes clés du processus de création de la tâche : lorsque vous consultez le tableau des compartiments S3 que vous avez sélectionnés pour la tâche (étape 2) et lorsque vous passez en revue tous les paramètres de la tâche (étape 8). Ces estimations peuvent vous aider à déterminer s'il convient d'ajuster les paramètres de la tâche avant de l'enregistrer. La disponibilité et la nature des estimations dépendent des paramètres que vous choisissez pour la tâche.

Révision des coûts estimés pour chaque compartiment (étape 2)

Si vous sélectionnez explicitement des compartiments individuels pour une tâche à analyser, vous pouvez consulter le coût estimé de l'analyse des objets dans chacun de ces compartiments. Macie affiche ces estimations à l'étape 2 du processus de création d'emplois, lorsque vous passez en revue vos sélections de compartiments. Dans le tableau de cette étape, le champ Estimated cost (Coût estimé) indique le coût estimatif total (en dollars américains) de l'exécution de la tâche pour analyser les objets d'un compartiment.

Chaque estimation reflète la quantité projetée de données non compressées que la tâche analysera dans un bucket, en fonction de la taille et des types d'objets actuellement stockés dans le bucket. L'estimation reflète également les prix de Macie pour le courantRégion AWS.

Seuls les objets classifiables sont inclus dans l'estimation du coût d'un bucket. Un objet classifiable est un objet S3 qui utilise une classe de stockage prise en charge Amazon S3 et possède une extension de nom de fichier pour un fichier ou un format de stockage pris en charge. Si des objets classifiables sont des fichiers compressés ou archivés, l'estimation suppose que les fichiers utilisent un taux de compression de 3:1 et que la tâche peut analyser tous les fichiers extraits.

Révision du coût total estimé d'un travail (étape 8)

Si vous créez une tâche ponctuelle ou si vous créez et configurez une tâche périodique pour inclure des objets S3 existants, Macie calcule et affiche le coût total estimé de la tâche au cours de la dernière étape du processus de création de la tâche. Vous pouvez consulter cette estimation tout en passant en revue et en vérifiant tous les paramètres que vous avez sélectionnés pour la tâche.

Cette estimation indique le coût total prévu (en dollars américains) de l'exécution de la tâche une fois dans la région actuelle. L'estimation reflète la quantité prévue de données non compressées que la tâche analysera. Il est basé sur la taille et les types d'objets qui sont actuellement stockés dans des compartiments que vous avez explicitement sélectionnés pour la tâche ou jusqu'à 500 compartiments qui correspondent actuellement aux critères de compartiment que vous avez spécifiés pour la tâche, en fonction des paramètres de la tâche.

Notez que cette estimation ne reflète aucune des options que vous avez sélectionnées pour affiner et réduire l'étendue de la tâche, par exemple, une profondeur d'échantillonnage plus faible ou des critères excluant certains objets S3 de la tâche. Il ne reflète pas non plus votre quota mensuel de découverte de données sensibles, qui peut limiter la portée et le coût de l'analyse de la tâche, ni les remises pouvant s'appliquer à votre compte.

Outre le coût total estimé du travail, l'estimation fournit des données agrégées qui offrent un aperçu de l'étendue et du coût prévus du travail :

- Les valeurs de taille indiquent la taille de stockage totale des objets que la tâche peut et ne peut pas analyser.
- Les valeurs du nombre d'objets indiquent le nombre total d'objets que la tâche peut et ne peut pas analyser.

Dans ces valeurs, un objet classifiable est un objet S3 qui utilise une classe de stockage Amazon S3 prise en charge et possède une extension de nom de fichier pour un fichier ou un format de stockage pris en charge. Seuls les objets classifiables sont inclus dans l'estimation des coûts. Un objet non classifiable est un objet qui n'utilise pas de classe de stockage prise en charge ou ne possède pas d'extension de nom de fichier pour un fichier ou un format de stockage pris en charge. Ces objets ne sont pas inclus dans l'estimation des coûts.

L'estimation fournit des données agrégées supplémentaires pour les objets S3 qui sont des fichiers compressés ou archivés. La valeur Compressed (Compressed value) indique la taille de stockage totale des objets qui utilisent une classe de stockage prise en charge Amazon S3 et possèdent une extension de nom de fichier pour un type de fichier compressé ou d'archive

pris en charge. La valeur non compressée indique la taille approximative de ces objets s'ils sont décompressés, en fonction d'un taux de compression spécifié. Ces données sont pertinentes en raison de la façon dont Macie analyse les fichiers compressés et les fichiers d'archive.

Lorsque Macie analyse un fichier compressé ou d'archive, elle inspecte à la fois le fichier complet et son contenu. Pour inspecter le contenu du fichier, Macie décompresse le fichier, puis inspecte chaque fichier extrait utilisant un format compatible. La quantité réelle de données qu'une tâche analyse dépend donc de :

- Si un fichier utilise la compression et, dans l'affirmative, quel est le taux de compression qu'il utilise.
- Le nombre, la taille et le format des fichiers extraits.

Par défaut, Macie part des hypothèses suivantes lorsqu'elle calcule les estimations de coûts pour une tâche :

- Tous les fichiers compressés et archivés utilisent un taux de compression de 3:1.
- Tous les fichiers extraits utilisent un format de fichier ou de stockage compatible.

Ces hypothèses peuvent donner lieu à une estimation plus importante de l'étendue des données que la tâche analysera et, par conséquent, à une estimation des coûts plus élevée pour la tâche.

Vous pouvez recalculer le coût total estimé de la tâche en fonction d'un taux de compression différent. Pour ce faire, choisissez le ratio dans la liste Choisissez un taux de compression estimé de la section Coût estimé. Macie met ensuite à jour l'estimation pour qu'elle corresponde à votre sélection.

Pour plus d'informations sur la manière dont Macie calcule les coûts estimés, consultez. Comprendre comment les coûts d'utilisation estimés sont calculés

Surveillance des coûts estimés pour les tâches de découverte de données sensibles

Si vous exécutez déjà des tâches de découverte de données sensibles, la page Utilisation de la console Amazon Macie peut vous aider à contrôler le coût estimé de ces tâches. La page affiche vos coûts estimés (en dollars américains) pour l'utilisation de Macie au Région AWS cours du mois civil en cours. Pour plus d'informations sur la façon dont Macie calcule ces estimations, reportez-vous à la section. Comprendre comment les coûts d'utilisation estimés sont calculés

Pour consulter vos coûts estimatifs liés à l'exécution de tâches

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.

2. À l'aide du Région AWS sélecteur dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous voulez consulter vos coûts estimés.
3. Dans le panneau de navigation, choisissez Utilisation.
4. Sur la page Utilisation, consultez la ventilation des coûts estimés pour votre compte. L'élément Tâches de découverte de données sensibles indique le coût total estimé des tâches que vous avez exécutées jusqu'ici au cours du mois en cours dans la région en cours.

   Si vous êtes l'administrateur Macie d'une organisation, la section Coûts estimés indique les coûts estimés pour l'ensemble de votre organisation pour le mois en cours dans la région en cours. Pour afficher le coût estimatif total des tâches exécutées pour un compte membre membre membre membre membre, choisissez le compte dans le tableau. La section Coûts estimés affiche ensuite une ventilation des coûts estimés pour le compte, y compris le coût estimé des tâches exécutées. Pour afficher ces données pour un autre compte, sélectionnez le compte dans le tableau. Pour effacer votre sélection de compte, choisissez X en regard de l'ID de compte.

Pour vérifier et contrôler vos coûts réels, utilisez AWS Billing and Cost Management.

Identificateurs de données gérés recommandés pour les tâches de découverte de données sensibles

Pour optimiser les résultats de vos tâches de découverte de données sensibles, vous pouvez configurer des tâches individuelles afin d'utiliser automatiquement l'ensemble d'identifiants de données gérés que nous recommandons pour les tâches. UNidentifiant de données géréesest un ensemble de critères et de techniques intégrés conçus pour détecter un type spécifique de données sensibles, par exemple,AWSles clés d'accès secrètes, les numéros de carte de crédit ou les numéros de passeport d'un pays ou d'une région en particulier.

L'ensemble recommandé d'identifiants de données gérés est conçu pour détecter les catégories et types courants de données sensibles. Sur la base de nos recherches, il peut détecter des catégories générales et des types de données sensibles tout en optimisant les résultats de votre travail en réduisant le bruit. À mesure que nous publions de nouveaux identifiants de données gérées, nous les ajoutons à cet ensemble s'ils sont susceptibles d'optimiser davantage les résultats de vos tâches. Au fil du temps, nous pouvons également ajouter ou supprimer des identifiants de données gérés existants de l'ensemble. Si nous ajoutons ou supprimons un identifiant de données gérées de l'ensemble recommandé, nous mettons à jour cette page pour indiquer la nature et le moment de la modification. Pour recevoir des alertes automatiques concernant ces modifications, vous pouvez vous abonner au fil RSS surHistorique des documents Maciepage.

Lorsque vous créez une tâche de découverte de données sensibles, vous spécifiez les identifiants de données gérées que vous souhaitez que la tâche utilise pour analyser les objets dans les compartiments Amazon Simple Storage Service (Amazon S3). Pour configurer une tâche afin d'utiliser l'ensemble recommandé d'identificateurs de données gérés, choisissezRecommandéoption lorsque vous créez la tâche. La tâche utilise alors automatiquement tous les identificateurs de données gérées figurant dans l'ensemble recommandé lorsque la tâche commence à s'exécuter. Si vous configurez une tâche pour qu'elle s'exécute plusieurs fois, chaque exécution utilise automatiquement tous les identificateurs de données gérés qui figurent dans l'ensemble recommandé au démarrage de l'exécution.

Les rubriques suivantes répertorient les identifiants de données gérés qui figurent actuellement dans l'ensemble recommandé, organisés par catégorie et type de données sensibles. Ils spécifient l'identifiant unique (ID) pour chaque identifiant de données gérées de l'ensemble. Cet ID décrit le type de données sensibles qu'un identifiant de données gérées est conçu pour détecter, par exemple :`PGP_PRIVATE_KEY`pour les clés privées PGP et`USA_PASSPORT_NUMBER`pour les numéros de passeports américains.

Rubriques

- Informations d'identification
- Informations financières
- données d'identification personnelle (PII)
- Mises à jour de l'ensemble recommandé

Pour plus de détails sur des identifiants de données gérés spécifiques ou pour obtenir la liste complète de tous les identifiants de données gérés actuellement fournis par Macie, voirUtilisation des identificateurs de données gérés.

Informations d'identification

Pour détecter les occurrences de données d'identification dans les objets S3, l'ensemble recommandé utilise les identifiants de données gérés suivants.

Type de données sensibles	ID d'identifiant de données géré
Clé d'accès secrète AWS	`AWS_CREDENTIALS`
En-tête d'autorisation HTTP de base	`HTTP_BASIC_AUTH_HEADER`

Type de données sensibles	ID d'identifiant de données géré
Clé privée OpenSSH	`OPENSSH_PRIVATE_KEY`
Clé privée PGP	`PGP_PRIVATE_KEY`
Clé privée PKCS (Public Key Cryptography Standard)	`PKCS`
Clé privée PuTTY	`PUTTY_PRIVATE_KEY`

Informations financières

Pour détecter les occurrences d'informations financières dans les objets S3, l'ensemble recommandé utilise les identifiants de données gérés suivants.

Type de données sensibles	ID d'identifiant de données géré
Données de la bande magnétique des cartes de crédit	`CREDIT_CARD_MAGNETIC_STRIPE`
Numéro de carte de crédit	`CREDIT_CARD_NUMBER` (pour les numéros de carte de crédit à proximité d'un mot clé)

données d'identification personnelle (PII)

Pour détecter les occurrences d'informations personnelles identifiables (PII) dans les objets S3, l'ensemble recommandé utilise les identifiants de données gérés suivants.

Type de données sensibles	ID d'identifiant de données géré
Numéro d'identification du permis de conduire	`CANADA_DRIVERS_LICENSE, DRIVERS_LICENSE` (pour les États-Unis),`UK_DRIVERS_LICENSE`
Numéro de liste électorale	`UK_ELECTORAL_ROLL_NUMBER`

Type de données sensibles	ID d'identifiant de données géré
Numéro d'identification nationale	`FRANCE_NATIONAL_IDENTIFICATION_NUMBER, GERMANY_NATIONAL_IDENTIFICATION_NUMBER, ITALY_NATIONAL_IDENTIFICATION_NUMBER, SPAIN_DNI_NUMBER`
Numéro d'assurance nationale (NINO)	`UK_NATIONAL_INSURANCE_NUMBER`
Numéro de passeport	`CANADA_PASSPORT_NUMBER, FRANCE_PASSPORT_NUMBER, GERMANY_PASSPORT_NUMBER, ITALY_PASSPORT_NUMBER, SPAIN_PASSPORT_NUMBER, UK_PASSPORT_NUMBER, USA_PASSPORT_NUMBER`
Numéro de sécurité sociale	`CANADA_SOCIAL_INSURANCE_NUMBER`
Numéro de sécurité sociale	`SPAIN_SOCIAL_SECURITY_NUMBER, USA_SOCIAL_SECURITY_NUMBER`
Numéro d'identification ou de référence du contribuable	`AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER`

Mises à jour de l'ensemble recommandé

Le tableau suivant décrit les modifications apportées à l'ensemble d'identifiants de données gérés que nous recommandons pour les tâches de découverte de données sensibles. Pour recevoir des

alertes automatiques concernant ces modifications, abonnez-vous au fil RSS duHistorique des documents Maciepage.

Modification	Description	Date
Disponibilité générale	Version initiale du kit recommandé.	27 juin 2023

Analyse d'objets Amazon S3 chiffrés avec Amazon Macie

Lorsque vous activez Amazon Macie pour votre compte Compte AWS, Macie crée un rôle lié à un service qui lui accorde les autorisations nécessaires pour appeler Amazon Simple Storage Service (Amazon S3) et d'autres personnes en votre nom. Services AWS Un rôle lié à un service simplifie le processus de configuration Service AWS car vous n'avez pas à ajouter manuellement des autorisations pour que le service puisse effectuer des actions en votre nom. Pour en savoir plus sur ce type de rôle, consultez la section Utilisation des rôles liés à un service dans le Guide de l'AWS Identity and Access Management utilisateur.

La politique d'autorisation pour le rôle lié au service Macie (`AWSServiceRoleForAmazonMacie`) permet à Macie d'effectuer des actions qui incluent la récupération d'informations sur vos compartiments et objets S3, ainsi que la récupération et l'analyse d'objets dans vos compartiments S3. Si votre compte est le compte administrateur Macie d'une organisation, la politique permet également à Macie d'effectuer ces actions en votre nom pour les comptes des membres de votre organisation.

Si un objet S3 est chiffré, la politique d'autorisation pour le rôle lié au service Macie accorde généralement à Macie les autorisations dont il a besoin pour déchiffrer l'objet. Cela dépend toutefois du type de chiffrement utilisé. Cela peut également dépendre de l'autorisation de Macie à utiliser la clé de chiffrement appropriée.

Rubriques

- Options de chiffrement pour les objets Amazon S3
- Autoriser Amazon Macie à utiliser un service géré par le client AWS KMS key

Options de chiffrement pour les objets Amazon S3

Amazon S3 prend en charge plusieurs options de chiffrement pour les objets S3. Pour la plupart de ces options, Amazon Macie peut déchiffrer un objet en utilisant le rôle lié au service Macie pour votre compte. Cela dépend toutefois du type de chiffrement utilisé pour chiffrer un objet.

Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)

Si un objet est chiffré à l'aide d'un chiffrement côté serveur avec une clé gérée Amazon S3 (SSE-S3), Macie peut déchiffrer l'objet.

Pour en savoir plus sur ce type de chiffrement, consultez la section Utilisation du chiffrement côté serveur avec des clés gérées par Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Chiffrement côté serveur avec AWS KMS keys (DSSE-KMS et SSE-KMS)

Si un objet est chiffré à l'aide d'un chiffrement double couche côté serveur ou d'un chiffrement côté serveur avec un système AWS géré AWS KMS key (DSSE-KMS ou SSE-KMS), Macie peut déchiffrer l'objet.

Si un objet est chiffré à l'aide d'un chiffrement double couche côté serveur ou d'un chiffrement côté serveur géré par le client AWS KMS key (DSSE-KMS ou SSE-KMS), Macie ne peut déchiffrer l'objet que si vous autorisez Macie à utiliser la clé. C'est le cas pour les objets chiffrés avec des clés KMS entièrement gérées dans un magasin de clés externe AWS KMS et des clés KMS dans un magasin de clés externe. Si Macie n'est pas autorisé à utiliser la clé KMS applicable, Macie peut uniquement stocker et signaler les métadonnées de l'objet.

Pour en savoir plus sur ces types de chiffrement, consultez les sections Utilisation du chiffrement double couche côté serveur avec AWS KMS keys et Utilisation du chiffrement côté serveur avec dans AWS KMS keys le guide de l'utilisateur d'Amazon Simple Storage Service.

> **Tip**
>
> Vous pouvez générer automatiquement une liste de tous les clients gérés AWS KMS keys auxquels Macie doit accéder pour analyser des objets dans des compartiments S3 pour votre compte. Pour ce faire, exécutez le script AWS KMS Permission Analyzer, disponible dans le référentiel Amazon Macie Scripts sur. GitHub Le script peut également générer un script supplémentaire de commandes AWS Command Line Interface (AWS CLI). Vous

pouvez éventuellement exécuter ces commandes pour mettre à jour les paramètres de configuration et les politiques requis pour les clés KMS que vous spécifiez.

Chiffrement côté serveur avec des clés fournies par le client (SSE-C)

Si un objet est chiffré à l'aide d'un chiffrement côté serveur avec une clé fournie par le client (SSE-C), Macie ne peut pas déchiffrer l'objet. Macie peut uniquement stocker et rapporter les métadonnées de l'objet.

Pour en savoir plus sur ce type de chiffrement, consultez la section Utilisation du chiffrement côté serveur avec des clés fournies par le client dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Chiffrement côté client

Si un objet est chiffré à l'aide du chiffrement côté client, Macie ne peut pas le déchiffrer. Macie peut uniquement stocker et rapporter les métadonnées de l'objet. Par exemple, Macie peut indiquer la taille de l'objet et les balises associées à l'objet.

Pour en savoir plus sur ce type de chiffrement dans le contexte d'Amazon S3, consultez la section Protection des données à l'aide du chiffrement côté client dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Vous pouvez filtrer l'inventaire de vos compartiments dans Macie afin de déterminer quels compartiments S3 stockent des objets utilisant certains types de chiffrement. Vous pouvez également déterminer quels compartiments utilisent certains types de chiffrement côté serveur par défaut lors du stockage de nouveaux objets. Le tableau suivant fournit des exemples de filtres que vous pouvez appliquer à votre inventaire de compartiments pour trouver ces informations.

Pour montrer des seaux qui...	Appliquer ce filtre...
Stockez les objets qui utilisent le chiffrement SSE-C	Le nombre d'objets par chiffrement est fourni par le client et From = 1
Stockez les objets qui utilisent le chiffrement DSSE-KMS ou SSE-KMS	Le nombre d'objets par chiffrement est AWS KMS géré et From = 1

Pour montrer des seaux qui...	Appliquer ce filtre...
Stockez les objets qui utilisent le chiffrement SSE-S3	Le nombre d'objets par chiffrement est géré par Amazon S3 et From = 1
Stockez les objets qui utilisent le chiffrement côté client (ou qui ne sont pas chiffrés)	Le nombre d'objets par chiffrement est « Aucun chiffrement » et « From » = 1
Chiffrez les nouveaux objets par défaut à l'aide du chiffrement DSSE-KMS	Chiffrement par défaut = aws:kms:dsse
Chiffrez les nouveaux objets par défaut à l'aide du chiffrement SSE-KMS	Chiffrement par défaut = aws:kms
Chiffrez les nouveaux objets par défaut à l'aide du chiffrement SSE-S3	Chiffrement par défaut = AES256

Si un bucket est configuré pour chiffrer de nouveaux objets par défaut à l'aide du chiffrement DSSE-KMS ou SSE-KMS, vous pouvez également déterminer lequel est utilisé. AWS KMS key Pour ce faire, choisissez le compartiment sur la page des compartiments S3. Dans le panneau des détails du bucket, sous Chiffrement côté serveur, reportez-vous au AWS KMS keychamp. Ce champ indique le nom de ressource Amazon (ARN) ou l'identifiant unique (ID de clé) de la clé.

Autoriser Amazon Macie à utiliser un service géré par le client AWS KMS key

Si un objet Amazon S3 est chiffré à l'aide d'un chiffrement double couche côté serveur ou d'un chiffrement côté serveur géré par le client AWS KMS key (DSSE-KMS ou SSE-KMS), Amazon Macie ne peut déchiffrer l'objet que s'il est autorisé à utiliser la clé. La manière de fournir cet accès dépend du fait que le compte propriétaire de la clé possède également le compartiment S3 qui stocke l'objet :

- Si le même compte possède le bucket AWS KMS key et le bucket, un utilisateur du compte doit mettre à jour la politique de la clé.
- Si un compte possède le compartiment AWS KMS key et qu'un autre compte possède le compartiment, un utilisateur du compte propriétaire de la clé doit autoriser l'accès entre comptes à la clé.

Cette rubrique décrit comment effectuer ces tâches et fournit des exemples pour les deux scénarios. Pour en savoir plus sur l'autorisation d'accès aux services gérés par le client AWS KMS keys, consultez la section Authentification et contrôle d'accès AWS KMS dans le guide du AWS Key Management Service développeur.

Permettre à un même compte d'accéder à une clé gérée par le client

Si le même compte possède à la fois le compartiment S3 AWS KMS key et le compartiment S3, un utilisateur du compte doit ajouter une déclaration à la politique relative à la clé. La déclaration supplémentaire doit autoriser le rôle lié au service Macie du compte à déchiffrer les données à l'aide de la clé. Pour obtenir des informations détaillées sur la mise à jour d'une politique clé, consultez la section Modification d'une politique clé dans le Guide du AWS Key Management Service développeur.

Dans la déclaration :

- L'`Principal`élément doit spécifier le nom de ressource Amazon (ARN) du rôle lié au service Macie pour le compte propriétaire du compartiment AWS KMS key et du compartiment S3.

  Si le compte est opt-in Région AWS, l'ARN doit également inclure le code de région approprié pour la région. Par exemple, si le compte se trouve dans la région Moyen-Orient (Bahreïn), dont le code de région est me-south-1, `Principal` l'élément doit `arn:aws:iam::`*`123456789012`*`:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie` spécifier, *où* 123456789012 est l'identifiant du compte. Pour obtenir la liste des codes régionaux des régions dans lesquelles Macie est actuellement disponible, consultez la section Points de terminaison et quotas Amazon Macie dans le. Références générales AWS
- Le `Action` tableau doit spécifier l'`kms:Decrypt`action. C'est la seule AWS KMS action que Macie doit être autorisée à effectuer pour déchiffrer un objet S3 chiffré avec la clé.

Voici un exemple de déclaration à ajouter à la politique pour un AWS KMS key.

```
{
    "Sid": "Allow the Macie service-linked role to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie"
    },
```

```
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

Dans l'exemple précédent :

- Le `AWS` champ de l'`Principal`élément indique l'ARN du rôle lié au service Macie (`AWSServiceRoleForAmazonMacie`) pour le compte. Cela permet au rôle lié au service Macie d'effectuer l'action spécifiée par la déclaration de politique. *`123456789012`* est un exemple d'ID de compte. Remplacez cette valeur par l'ID de compte du compte propriétaire de la clé KMS et du compartiment S3.
- Le `Action` tableau indique l'action que le rôle lié au service Macie est autorisé à effectuer à l'aide de la clé KMS : déchiffrer le texte chiffré avec la clé.

L'endroit où vous ajoutez cette déclaration à une politique clé dépend de la structure et des éléments que la stratégie contient actuellement. Lorsque vous ajoutez l'instruction, assurez-vous que la syntaxe est valide. Les politiques clés utilisent le format JSON. Cela signifie que vous devez également ajouter une virgule avant ou après la déclaration, selon l'endroit où vous ajoutez la déclaration à la politique.

Autoriser l'accès entre comptes à une clé gérée par le client

Si un compte possède le AWS KMS key (propriétaire de la clé) et qu'un autre compte possède le compartiment S3 (propriétaire du compartiment), le propriétaire de la clé doit fournir au propriétaire du compartiment un accès multicompte à la clé KMS. Pour ce faire, le propriétaire de la clé s'assure d'abord que la politique de la clé autorise le propriétaire du compartiment à utiliser la clé et à créer une autorisation pour la clé. Le propriétaire du compartiment crée ensuite une subvention pour la clé. Une subvention est un instrument de politique qui permet AWS aux principaux d'utiliser des clés KMS dans des opérations cryptographiques si les conditions spécifiées par la subvention sont remplies. Dans ce cas, la subvention délègue les autorisations pertinentes au rôle lié au service Macie pour le compte du propriétaire du bucket.

Pour obtenir des informations détaillées sur la mise à jour d'une politique clé, consultez la section Modification d'une politique clé dans le Guide du AWS Key Management Service développeur. Pour en savoir plus sur les subventions, consultez la section Subventions AWS KMS dans le guide du AWS Key Management Service développeur.

Étape 1 : Mettre à jour la politique clé

Dans la politique clé, le propriétaire de la clé doit s'assurer qu'elle inclut deux déclarations :

- La première instruction permet au propriétaire du compartiment d'utiliser la clé pour déchiffrer les données.
- La deuxième déclaration permet au propriétaire du compartiment de créer une subvention pour le rôle lié au service Macie pour son compte (celui du propriétaire du compartiment).

Dans la première instruction, l'`Principal`élément doit spécifier l'ARN du compte du propriétaire du bucket. Le `Action` tableau doit spécifier l'`kms:Decrypt`action. C'est la seule AWS KMS action que Macie doit être autorisée à effectuer pour déchiffrer un objet chiffré avec la clé. Voici un exemple de cette déclaration dans la politique d'un AWS KMS key.

```
{
    "Sid": "Allow account 111122223333 to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

Dans l'exemple précédent :

- Le AWS champ de l'`Principal`élément indique l'ARN du compte du propriétaire du compartiment (*111122223333*). Il permet au propriétaire du compartiment d'effectuer l'action spécifiée par la déclaration de politique. *111122223333* est un exemple d'ID de compte. Remplacez cette valeur par l'ID du compte du propriétaire du compartiment.
- Le `Action` tableau indique l'action que le propriétaire du compartiment est autorisé à effectuer à l'aide de la clé KMS : déchiffrer le texte chiffré avec la clé.

La deuxième déclaration de la politique clé permet au propriétaire du compartiment de créer une subvention pour le rôle lié au service Macie pour son compte. Dans cette déclaration, l'`Principal`élément doit spécifier l'ARN du compte du propriétaire du bucket. Le `Action`

tableau doit spécifier l'`kms:CreateGrant`action. Un `Condition` élément peut filtrer l'accès à l'`kms:CreateGrant`action spécifiée dans l'instruction. Voici un exemple de cette déclaration dans la politique d'un AWS KMS key.

```
{
    "Sid": "Allow account 111122223333 to create a grant",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie"
        }
    }
}
```

Dans l'exemple précédent :

- Le AWS champ de l'`Principal`élément indique l'ARN du compte du propriétaire du compartiment (*111122223333*). Il permet au propriétaire du compartiment d'effectuer l'action spécifiée par la déclaration de politique. *111122223333* est un exemple d'ID de compte. Remplacez cette valeur par l'ID du compte du propriétaire du compartiment.
- Le `Action` tableau indique l'action que le propriétaire du compartiment est autorisé à effectuer sur la clé KMS : créer une autorisation pour la clé.
- L'`Condition`élément utilise l'opérateur de `StringEquals` condition et la clé de `kms:GranteePrincipal` condition pour filtrer l'accès à l'action spécifiée par la déclaration de politique. Dans ce cas, le propriétaire du bucket peut créer une subvention uniquement pour le paramètre spécifié`GranteePrincipal`, à savoir l'ARN du rôle lié au service Macie associé à son compte. Dans cet ARN, *111122223333* est un exemple d'ID de compte. Remplacez cette valeur par l'ID du compte du propriétaire du compartiment.

  Si le compte du propriétaire du bucket est activé Région AWS, incluez également le code de région approprié dans l'ARN du rôle lié au service Macie. Par exemple, si le compte se trouve dans la région Moyen-Orient (Bahreïn), dont le code de région est me-south-1, `macie.amazonaws.com`

remplacez-le par `macie.me-south-1.amazonaws.com` dans l'ARN. Pour obtenir la liste des codes régionaux des régions dans lesquelles Macie est actuellement disponible, consultez la section Points de terminaison et quotas Amazon Macie dans le. Références générales AWS

L'endroit où le propriétaire de la clé ajoute ces déclarations à la politique clé dépend de la structure et des éléments que la politique contient actuellement. Lorsque le propriétaire de la clé ajoute les instructions, il doit s'assurer que la syntaxe est valide. Les politiques clés utilisent le format JSON. Cela signifie que le propriétaire de la clé doit également ajouter une virgule avant ou après chaque instruction, selon l'endroit où il ajoute l'instruction à la politique.

Étape 2 : Création d'une subvention

Une fois que le propriétaire de la clé a mis à jour la politique des clés si nécessaire, le propriétaire du compartiment doit créer une autorisation pour la clé. La subvention délègue les autorisations pertinentes au rôle lié au service Macie pour leur compte (celui du propriétaire du bucket). Avant que le propriétaire du bucket ne crée la subvention, il doit vérifier qu'il est autorisé à effectuer l'`kms:CreateGrant`action pour son compte. Cette action leur permet d'ajouter une subvention à une subvention existante gérée par le client AWS KMS key.

Pour créer la subvention, le propriétaire du bucket peut utiliser le CreateGrantfonctionnement de l' AWS Key Management Service API. Lorsque le propriétaire du bucket crée l'autorisation, il doit spécifier les valeurs suivantes pour les paramètres requis :

- `KeyId`— L'ARN de la clé KMS. Pour un accès entre comptes à une clé KMS, cette valeur doit être un ARN. Il ne peut pas s'agir d'un identifiant clé.
- `GranteePrincipal`— L'ARN du rôle lié au service Macie (`AWSServiceRoleForAmazonMacie`) pour leur compte. Cette valeur doit être`arn:aws:iam::`*`111122223333`*`:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`, où *`111122223333`* est l'ID de compte du propriétaire du compartiment.

  Si leur compte se trouve dans une région optionnelle, l'ARN doit inclure le code de région approprié. Par exemple, si leur compte se trouve dans la région Moyen-Orient (Bahreïn), dont le code de région est me-south-1, l'ARN doit `arn:aws:iam::`*`111122223333`*`:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie` être, *où* 111122223333 est l'identifiant du compte du propriétaire du compartiment.
- `Operations`— L'action de AWS KMS déchiffrement (`Decrypt`). C'est la seule AWS KMS action que Macie doit être autorisée à effectuer pour déchiffrer un objet chiffré avec la clé KMS.

Pour créer une autorisation pour une clé KMS gérée par le client à l'aide de la AWS Command Line Interface (AWS CLI), exécutez la commande create-grant. L'exemple suivant montre comment procéder. L'exemple est formaté pour Microsoft Windows et utilise le caractère de continuation de ligne caret (^) pour améliorer la lisibilité.

```
C:\> aws kms create-grant ^
--key-id arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab ^
--grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
macie.amazonaws.com/AWSServiceRoleForAmazonMacie ^
--operations "Decrypt"
```

Où :

- `key-id`spécifie l'ARN de la clé KMS à laquelle appliquer l'autorisation.
- `grantee-principal`spécifie l'ARN du rôle lié au service Macie pour le compte autorisé à effectuer l'action spécifiée par la subvention. Cette valeur doit correspondre à l'ARN spécifié par la `kms:GranteePrincipal` condition de la deuxième instruction de la politique clé.
- `operations`spécifie l'action que l'autorisation autorise le principal spécifié à effectuer : déchiffrer le texte chiffré avec la clé KMS.

Si la commande s'exécute correctement, vous recevez une sortie similaire à ce qui suit.

```
{
    "GrantToken": "<grant token>",
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

Où se `GrantToken` trouve une chaîne unique, non secrète, de longueur variable, codée en base64 qui représente la subvention créée et `GrantId` constitue l'identifiant unique de la subvention.

Stockage et conservation des résultats de découverte de données sensibles avec Amazon Macie

Lorsque vous exécutez une tâche de découverte de données sensibles ou qu'Amazon Macie effectue une découverte automatique de données sensibles, Macie crée un enregistrement d'analyse pour chaque objet Amazon Simple Storage Service (Amazon S3) inclus dans le périmètre de l'analyse.

Ces enregistrements, appelés résultats de découverte de données sensibles, enregistrent les détails de l'analyse que Macie effectue sur des objets S3 individuels. Cela inclut les objets dans lesquels Macie ne détecte pas de données sensibles et ne produit donc pas de résultats, ainsi que les objets que Macie ne peut pas analyser en raison d'erreurs ou de problèmes. Si Macie détecte des données sensibles dans un objet, l'enregistrement inclut les données de la découverte correspondante ainsi que des informations supplémentaires. Les résultats de découverte de données sensibles vous fournissent des enregistrements d'analyse qui peuvent être utiles pour les audits ou les enquêtes sur la confidentialité et la protection des données.

Macie conserve les résultats de la découverte de vos données sensibles pendant 90 jours seulement. Pour accéder à vos résultats et permettre leur stockage et leur conservation à long terme, configurez Macie pour chiffrer les résultats avec une clé AWS Key Management Service (AWS KMS) et les stocker dans un compartiment S3. Le bucket peut servir de référentiel définitif à long terme pour tous vos résultats de découverte de données sensibles. Vous pouvez ensuite éventuellement accéder aux résultats de ce référentiel et les interroger.

Cette rubrique vous explique comment utiliser le AWS Management Console pour configurer un référentiel pour vos résultats de découverte de données sensibles. La configuration est une combinaison d'un AWS KMS key qui chiffre les résultats, d'un compartiment S3 à usage général qui stocke les résultats et de paramètres Macie qui indiquent la clé et le compartiment à utiliser. Si vous préférez configurer les paramètres Macie par programmation, vous pouvez utiliser l'API PutClassificationExportConfigurationAmazon Macie.

Lorsque vous configurez les paramètres dans Macie, vos choix s'appliquent uniquement aux paramètres actuels Région AWS. Si vous êtes l'administrateur Macie d'une organisation, vos choix s'appliquent uniquement à votre compte. Ils ne s'appliquent pas aux comptes membres associés.

Si vous utilisez Macie à plusieurs reprises Régions AWS, configurez les paramètres du référentiel pour chaque région dans laquelle vous utilisez Macie. Vous pouvez éventuellement stocker les résultats de découverte de données sensibles pour plusieurs régions dans le même compartiment S3. Notez toutefois les exigences suivantes :

- Pour stocker les résultats d'une région AWS activée par défaut Comptes AWS, telle que la région USA Est (Virginie du Nord), vous devez choisir un compartiment dans une région activée par défaut. Les résultats ne peuvent pas être stockés dans un compartiment d'une région optionnelle (région désactivée par défaut).
- Pour stocker les résultats d'une région optionnelle, telle que la région du Moyen-Orient (Bahreïn), vous devez choisir un compartiment dans cette même région ou une région activée par défaut.

Les résultats ne peuvent pas être stockés dans un compartiment situé dans une autre région optionnelle.

Pour déterminer si une région est activée par défaut, consultez la section Régions et points de terminaison dans le guide de l'AWS Identity and Access Management utilisateur. Outre les exigences précédentes, déterminez également si vous souhaitez récupérer des échantillons de données sensibles que Macie rapporte dans des résultats individuels. Pour récupérer des échantillons de données sensibles d'un objet S3 concerné, toutes les ressources et données suivantes doivent être stockées dans la même région : l'objet concerné, le résultat applicable et le résultat de découverte de données sensibles correspondant.

Tâches

- Présentation
- Étape 1 : Vérifier vos autorisations
- Étape 2 : Configuration d'un AWS KMS key
- Étape 3 : Choisissez un compartiment S3

Présentation

Amazon Macie crée automatiquement un résultat de découverte de données sensibles pour chaque objet Amazon S3 qu'il analyse ou tente d'analyser lorsque vous exécutez une tâche de découverte de données sensibles ou qu'il effectue une découverte automatique de données sensibles. Cela consiste notamment à :

- Objets dans lesquels Macie détecte des données sensibles et, par conséquent, produisent également des résultats de données sensibles.
- Objets dans lesquels Macie ne détecte pas de données sensibles et ne produisent donc pas de résultats de données sensibles.
- Objets que Macie ne peut pas analyser en raison d'erreurs ou de problèmes tels que les paramètres d'autorisation ou l'utilisation d'un format de fichier ou de stockage non pris en charge.

Si Macie détecte des données sensibles dans un objet S3, le résultat de la découverte de données sensibles inclut les données issues de la recherche de données sensibles correspondante. Il fournit également des informations supplémentaires, telles que l'emplacement de pas moins de 1 000 occurrences de chaque type de données sensibles trouvées par Macie dans l'objet. Par exemple :

- Numéro de colonne et de ligne d'une cellule ou d'un champ dans un classeur Microsoft Excel, un fichier CSV ou un fichier TSV
- Le chemin d'accès à un champ ou à un tableau dans un fichier JSON ou JSON Lines
- Numéro de ligne d'une ligne dans un fichier texte non binaire autre qu'un fichier CSV, JSON, JSON Lines ou TSV, par exemple un fichier HTML, TXT ou XML
- Numéro de page d'une page dans un fichier Adobe Portable Document Format (PDF)
- L'index d'enregistrement et le chemin d'accès à un champ dans un enregistrement d'un conteneur d'objets Apache Avro ou d'un fichier Apache Parquet

Si l'objet S3 concerné est un fichier d'archive, tel qu'un fichier .tar ou .zip, le résultat de la découverte de données sensibles fournit également des données de localisation détaillées pour les occurrences de données sensibles dans des fichiers individuels que Macie a extraits de l'archive. Macie n'inclut pas ces informations dans les résultats de données sensibles pour les fichiers d'archive. Pour signaler les données de localisation, les résultats de découverte de données sensibles utilisent un schéma JSON standardisé.

Un résultat de découverte de données sensibles n'inclut pas les données sensibles trouvées par Macie. Il vous fournit plutôt un enregistrement d'analyse qui peut être utile pour les audits ou les enquêtes.

Macie conserve les résultats de la découverte de vos données sensibles pendant 90 jours. Vous ne pouvez pas y accéder directement depuis la console Amazon Macie ou via l'API Amazon Macie. Suivez plutôt les étapes décrites dans cette rubrique pour configurer Macie afin qu'il crypte vos résultats avec un AWS KMS key que vous spécifiez et qu'il stocke les résultats dans un compartiment S3 à usage général que vous spécifiez également. Macie écrit ensuite les résultats dans des fichiers JSON Lines (.jsonl), ajoute les fichiers au bucket sous forme de fichiers GNU Zip (.gz) et chiffre les données à l'aide du chiffrement SSE-KMS. Depuis le 8 novembre 2023, Macie signe également les objets S3 obtenus avec un code d'authentification de message basé sur le hachage (HMAC). AWS KMS key

Une fois que vous avez configuré Macie pour stocker les résultats de la découverte de vos données sensibles dans un compartiment S3, le compartiment peut servir de référentiel définitif à long terme pour les résultats. Vous pouvez ensuite éventuellement accéder aux résultats de ce référentiel et les interroger.

> **Tip**
>
> Pour un exemple détaillé et instructif de la manière dont vous pouvez interroger et utiliser les résultats de découverte de données sensibles pour analyser et signaler les risques potentiels liés à la sécurité des données, consultez le billet de blog Comment interroger et visualiser les résultats de découverte de données sensibles de Macie avec Amazon Athena et QuickSight Amazon AWS sur le blog sur la sécurité.
> Pour obtenir des exemples de requêtes Amazon Athena que vous pouvez utiliser pour analyser les résultats de découverte de données sensibles, consultez le référentiel Amazon Macie Results Analytics sur. GitHub Ce référentiel fournit également des instructions pour configurer Athena afin de récupérer et de déchiffrer vos résultats, ainsi que des scripts pour créer des tables pour les résultats.

Étape 1 : Vérifier vos autorisations

Avant de configurer un référentiel pour vos résultats de découverte de données sensibles, vérifiez que vous disposez des autorisations nécessaires pour chiffrer et stocker les résultats. Pour vérifier vos autorisations, utilisez AWS Identity and Access Management (IAM) pour examiner les politiques IAM associées à votre identité IAM. Comparez ensuite les informations contenues dans ces politiques à la liste suivante des actions que vous devez être autorisé à effectuer pour configurer le référentiel.

Amazon Macie

Pour Macie, vérifiez que vous êtes autorisé à effectuer l'action suivante :

`macie2:PutClassificationExportConfiguration`

Cette action vous permet d'ajouter ou de modifier les paramètres du référentiel dans Macie.

Amazon S3

Pour Amazon S3, vérifiez que vous êtes autorisé à effectuer les actions suivantes :

- `s3:CreateBucket`
- `s3:GetBucketLocation`
- `s3:ListAllMyBuckets`
- `s3:PutBucketAcl`
- `s3:PutBucketPolicy`

- `s3:PutBucketPublicAccessBlock`
- `s3:PutObject`

Ces actions vous permettent d'accéder à un compartiment S3 à usage général pouvant servir de référentiel et de le configurer.

AWS KMS

Pour utiliser la console Amazon Macie afin d'ajouter ou de modifier les paramètres du référentiel, vérifiez également que vous êtes autorisé à effectuer les actions suivantes : AWS KMS

- `kms:DescribeKey`
- `kms:ListAliases`

Ces actions vous permettent de récupérer et d'afficher les informations relatives AWS KMS keys à votre compte. Vous pouvez ensuite choisir l'une de ces clés pour chiffrer les résultats de la découverte de données sensibles.

Si vous envisagez d'en créer un nouveau AWS KMS key pour chiffrer les données, vous devez également être autorisé à effectuer les actions suivantes : `kms:CreateKey`kms:GetKeyPolicy, et`kms:PutKeyPolicy`.

Si vous n'êtes pas autorisé à effectuer les actions requises, demandez de l'aide à votre AWS administrateur avant de passer à l'étape suivante.

Étape 2 : Configuration d'un AWS KMS key

Après avoir vérifié vos autorisations, déterminez celle que AWS KMS key vous souhaitez que Macie utilise pour chiffrer les résultats de la découverte de vos données sensibles. La clé doit être une clé KMS de chiffrement symétrique gérée par le client et activée au même endroit Région AWS que le compartiment S3 dans lequel vous souhaitez stocker les résultats.

La clé peut être une clé existante AWS KMS key de votre propre compte ou une clé existante détenue AWS KMS key par un autre compte. Si vous souhaitez utiliser une nouvelle clé KMS, créez-la avant de continuer. Si vous souhaitez utiliser une clé existante détenue par un autre compte, obtenez l'Amazon Resource Name (ARN) de la clé. Vous devez saisir cet ARN lorsque vous configurez les paramètres du référentiel dans Macie. Pour plus d'informations sur la création et la révision des paramètres des clés KMS, consultez la section Gestion des clés dans le guide du AWS Key Management Service développeur.

> **Note**
>
> La clé peut se trouver AWS KMS key dans un magasin de clés externe. Cependant, la clé peut alors être plus lente et moins fiable qu'une clé entièrement gérée en interne AWS KMS. Vous pouvez réduire ce risque en stockant les résultats de la découverte de vos données sensibles dans un compartiment S3 configuré pour utiliser la clé comme clé de compartiment S3. Cela réduit le nombre de AWS KMS demandes à effectuer pour chiffrer les résultats de la découverte de données sensibles.
> Pour plus d'informations sur l'utilisation des clés KMS dans les magasins de clés externes, consultez la section Stockages de clés externes du manuel du AWS Key Management Service développeur. Pour plus d'informations sur l'utilisation des clés de compartiment S3, consultez la section Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Après avoir déterminé la clé KMS que vous souhaitez que Macie utilise, autorisez Macie à utiliser la clé. Sinon, Macie ne sera pas en mesure de chiffrer ou de stocker vos résultats dans le référentiel. Pour autoriser Macie à utiliser la clé, mettez à jour la politique de clé pour la clé. Pour obtenir des informations détaillées sur les politiques clés et la gestion de l'accès aux clés KMS, consultez la section Politiques clés du guide du AWS Key Management Service développeur. AWS KMS

Pour mettre à jour la politique clé

1. Ouvrez la AWS KMS console à l'adresse https://console.aws.amazon.com/kms.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Choisissez la clé que vous souhaitez que Macie utilise pour chiffrer les résultats de la découverte de données sensibles.
4. Dans l'onglet Stratégie de clé choisissez Modifier.
5. Copiez la déclaration suivante dans votre presse-papiers, puis ajoutez-la à la politique :

```
{
    "Sid": "Allow Macie to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "macie.amazonaws.com"
    },
    "Action": [
```

```
            "kms:GenerateDataKey",
            "kms:Encrypt"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "111122223333"
            },
            "ArnLike": {
                "aws:SourceArn": [
                    "arn:aws:macie2:Region:111122223333:export-configuration:*",
                    "arn:aws:macie2:Region:111122223333:classification-job/*"
                ]
            }
        }
}
```

> **Note**
>
> Lorsque vous ajoutez l'instruction à la stratégie, assurez-vous que la syntaxe est correcte. Les stratégies utilisent le format JSON. Cela signifie que vous devez également ajouter une virgule avant ou après la déclaration, en fonction de l'endroit où vous ajoutez la déclaration à la stratégie. Si vous ajoutez l'instruction en tant que dernière instruction, ajoutez une virgule après l'accolade de fermeture pour l'instruction précédente. Si vous l'ajoutez en tant que première instruction ou entre deux instructions existantes, ajoutez une virgule après l'accolade de fermeture de l'instruction.

6. Mettez à jour l'instruction avec les valeurs correctes pour votre environnement :

   - Dans les `Condition` champs, remplacez les valeurs d'espace réservé, où :
     - *111122223333* est l'identifiant de votre compte. Compte AWS
     - La *région* est Région AWS celle dans laquelle vous utilisez Macie et vous souhaitez autoriser Macie à utiliser la clé.

       Si vous utilisez Macie dans plusieurs régions et que vous souhaitez autoriser Macie à utiliser la clé dans d'autres régions, ajoutez des `aws:SourceArn` conditions pour chaque région supplémentaire. Par exemple :

       ```
       "aws:SourceArn": [
           "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
       ```

```
    "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
    "arn:aws:macie2:us-west-2:111122223333:export-configuration:*",
    "arn:aws:macie2:us-west-2:111122223333:classification-job/*"
]
```

Vous pouvez également autoriser Macie à utiliser la clé dans toutes les régions. Pour ce faire, remplacez la valeur de l'espace réservé par le caractère générique (*). Par exemple :

```
"aws:SourceArn": [
    "arn:aws:macie2:*:111122223333:export-configuration:*",
    "arn:aws:macie2:*:111122223333:classification-job/*"
]
```

- Si vous utilisez Macie dans une région optionnelle, ajoutez le code de région approprié à la valeur du champ. `Service` Par exemple, si vous utilisez Macie dans la région du Moyen-Orient (Bahreïn), dont le code de région est me-south-1, remplacez par. `macie.amazonaws.com` `macie.me-south-1.amazonaws.com` Pour obtenir la liste des régions dans lesquelles Macie est actuellement disponible et le code régional de chacune d'entre elles, consultez la section Points de terminaison et quotas Amazon Macie dans le. Références générales AWS

Notez que les `Condition` champs utilisent deux clés de condition globales IAM :

- aws : SourceAccount — Cette condition permet à Macie d'effectuer les actions spécifiées uniquement pour votre compte. Plus précisément, il détermine quel compte peut effectuer les actions spécifiées pour les ressources et les actions spécifiées par la `aws:SourceArn` condition.

  Pour permettre à Macie d'effectuer les actions spécifiées pour des comptes supplémentaires, ajoutez l'ID de compte de chaque compte supplémentaire à cette condition. Par exemple :

  ```
  "aws:SourceAccount": [111122223333,444455556666]
  ```

- aws : SourceArn — Cette condition empêche les autres d' Services AWS effectuer les actions spécifiées. Cela empêche également Macie d'utiliser la clé lors d'autres actions pour votre compte. En d'autres termes, cela permet à Macie de chiffrer des objets S3 avec la clé uniquement si : les objets sont des résultats de découverte de données sensibles, et les résultats concernent la découverte automatique de données sensibles ou des tâches de découverte de données sensibles créées par le compte spécifié dans la région spécifiée.

Pour permettre à Macie d'effectuer les actions spécifiées pour des comptes supplémentaires, ajoutez des ARN pour chaque compte supplémentaire à cette condition. Par exemple :

```
"aws:SourceArn": [
    "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
    "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
    "arn:aws:macie2:us-east-1:444455556666:export-configuration:*",
    "arn:aws:macie2:us-east-1:444455556666:classification-job/*"
]
```

Les comptes spécifiés par les `aws:SourceArn` conditions `aws:SourceAccount` et doivent correspondre.

Ces conditions permettent d'éviter que Macie ne soit utilisée comme une adjointe confuse lors de transactions avec AWS KMS. Bien que cela ne soit pas recommandé, vous pouvez supprimer ces conditions de la déclaration.

7. Lorsque vous avez terminé d'ajouter et de mettre à jour le relevé, choisissez Enregistrer les modifications.

Étape 3 : Choisissez un compartiment S3

Après avoir vérifié vos autorisations et les avoir AWS KMS key configurées, vous êtes prêt à spécifier le compartiment S3 que vous souhaitez utiliser comme référentiel pour les résultats de la découverte de vos données sensibles. Vous avez deux options :

- Utiliser un nouveau compartiment S3 créé par Macie : si vous choisissez cette option, Macie crée automatiquement un nouveau compartiment S3 à usage général dans le compartiment actuel Région AWS pour les résultats de votre découverte. Macie applique également une politique de compartiment au compartiment. La politique permet à Macie d'ajouter des objets au compartiment. Cela nécessite également que les objets soient chiffrés avec AWS KMS key ce que vous spécifiez, à l'aide du cryptage SSE-KMS. Pour consulter la politique, choisissez Afficher la politique sur la console Amazon Macie après avoir spécifié le nom du bucket et la clé KMS à utiliser.
- Utilisez un compartiment S3 existant que vous créez : si vous préférez stocker les résultats de votre découverte dans un compartiment S3 spécifique que vous créez, créez-le avant de continuer. Le godet doit être un godet à usage général. En outre, les paramètres et la politique du compartiment doivent permettre à Macie d'ajouter des objets au compartiment. Cette rubrique

explique les paramètres à vérifier et comment mettre à jour la politique. Il fournit également des exemples de déclarations à ajouter à la politique.

Les sections suivantes fournissent des instructions pour chaque option. Choisissez la section correspondant à l'option souhaitée.

Utilisez un nouveau compartiment S3 créé par Macie

Si vous préférez utiliser un nouveau compartiment S3 créé par Macie pour vous, la dernière étape du processus consiste à configurer les paramètres du référentiel dans Macie.

Pour configurer les paramètres du référentiel dans Macie

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, sous Paramètres, sélectionnez Résultats de découverte.
3. Sous Référentiel pour les résultats de découverte de données sensibles, choisissez Create bucket.
4. Dans le champ Créer un compartiment, entrez le nom du compartiment.

   Le nom doit être unique pour tous les compartiments S3. En outre, le nom ne peut être composé que de lettres minuscules, de chiffres, de points (.) et de tirets (-). Pour connaître les exigences de dénomination supplémentaires, consultez les règles de dénomination des compartiments dans le guide de l'utilisateur d'Amazon Simple Storage Service.
5. Développez la section Avancé.
6. (Facultatif) Pour spécifier un préfixe à utiliser dans le chemin d'accès à un emplacement du compartiment, entrez le préfixe dans la zone Préfixe du résultat de la découverte des données.

   Lorsque vous entrez une valeur, Macie met à jour l'exemple ci-dessous pour indiquer le chemin d'accès à l'emplacement du compartiment où il stockera les résultats de votre découverte.
7. Pour Bloquer tout accès public, choisissez Oui pour activer tous les paramètres de blocage de l'accès public pour le bucket.

   Pour plus d'informations sur ces paramètres, consultez la section Blocage de l'accès public à votre espace de stockage Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.
8. Sous Paramètres de chiffrement, spécifiez celui AWS KMS key que vous souhaitez que Macie utilise pour chiffrer les résultats :

- Pour utiliser une clé de votre propre compte, choisissez Sélectionner une clé de votre compte. Ensuite, dans la AWS KMS keyliste, choisissez la clé à utiliser. La liste affiche les clés KMS de chiffrement symétriques gérées par le client pour votre compte.
- Pour utiliser une clé détenue par un autre compte, choisissez Enter the ARN of a key from another account. Ensuite, dans le champ AWS KMS key ARN, entrez le nom de ressource Amazon (ARN) de la clé à utiliser, par exemple. **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**

9. Lorsque vous avez fini de saisir les paramètres, choisissez Enregistrer.

   Macie teste les paramètres pour vérifier qu'ils sont corrects. Si certains paramètres sont incorrects, Macie affiche un message d'erreur pour vous aider à résoudre le problème.

Après avoir enregistré les paramètres du référentiel, Macie ajoute au référentiel les résultats de découverte existants des 90 jours précédents. Macie commence également à ajouter de nouveaux résultats de découverte au référentiel.

Utiliser un compartiment S3 existant que vous créez

Si vous préférez stocker vos données sensibles, les résultats de découverte dans un compartiment S3 spécifique, vous devez créer et configurer le compartiment avant de configurer les paramètres dans Macie. Lorsque vous créez le bucket, tenez compte des exigences suivantes :

- Le godet doit être un godet à usage général. Il ne peut pas s'agir d'un bucket de répertoire.
- Si vous activez Object Lock pour le bucket, vous devez désactiver le paramètre de rétention par défaut pour cette fonctionnalité. Sinon, Macie ne pourra pas ajouter les résultats de votre découverte au bucket. Pour plus d'informations sur ce paramètre, consultez la section Utilisation de S3 Object Lock dans le guide de l'utilisateur d'Amazon Simple Storage Service.
- Pour stocker les résultats de votre découverte pour une région activée par défaut Comptes AWS, telle que la région USA Est (Virginie du Nord), le bucket doit se trouver dans une région activée par défaut. Les résultats ne peuvent pas être stockés dans un compartiment d'une région optionnelle (région désactivée par défaut).
- Pour stocker les résultats de votre découverte pour une région optionnelle, telle que la région du Moyen-Orient (Bahreïn), le bucket doit se trouver dans la même région ou dans une région activée par défaut. Les résultats ne peuvent pas être stockés dans un compartiment situé dans une autre région optionnelle.

Pour déterminer si une région est activée par défaut, consultez la section Régions et points de terminaison dans le guide de l'AWS Identity and Access Management utilisateur.

Après avoir créé le compartiment, mettez à jour la politique du compartiment pour permettre à Macie de récupérer des informations sur le compartiment et d'y ajouter des objets. Vous pouvez ensuite configurer les paramètres dans Macie.

Pour mettre à jour la politique de compartiment pour le compartiment

1. Ouvrez la console Amazon S3 sur https://console.aws.amazon.com/s3/.
2. Choisissez le compartiment dans lequel vous souhaitez stocker les résultats de votre découverte.
3. Choisissez l'onglet Permissions (Autorisations).
4. Dans la section Bucket policy (Politique de compartiment), sélectionnez Edit (Modifier).
5. Copiez l'exemple de stratégie suivant dans votre Presse-papiers :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Macie to use the GetBucketLocation operation",
            "Effect": "Allow",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:GetBucketLocation",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:macie2:Region:111122223333:export-
configuration:*",
                        "arn:aws:macie2:Region:111122223333:classification-job/*"
                    ]
                }
            }
        },
        {
```

```
            "Sid": "Allow Macie to add objects to the bucket",
            "Effect": "Allow",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:macie2:Region:111122223333:export-
configuration:*",
                        "arn:aws:macie2:Region:111122223333:classification-job/*"
                    ]
                }
            }
        },
        {
            "Sid": "Deny unencrypted object uploads. This is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-server-side-encryption": "aws:kms"
                }
            }
        },
        {
            "Sid": "Deny incorrect encryption headers. This is optional",
            "Effect": "Deny",
            "Principal": {
                "Service": "macie.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myBucketName/[optional prefix/]*",
            "Condition": {
                "StringNotEquals": {
```

```
                    "s3:x-amz-server-side-encryption-aws-kms-key-id":
 "arn:aws:kms:Region:111122223333:key/KMSKeyId"
                }
            }
        },
        {
            "Sid": "Deny non-HTTPS access",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::myBucketName/*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

6. Collez l'exemple de politique dans l'éditeur de politique Bucket sur la console Amazon S3.
7. Mettez à jour l'exemple de politique avec les valeurs correctes pour votre environnement :

   - Dans l'instruction facultative qui refuse les en-têtes de chiffrement incorrects :
     - Remplacez *myBucketName* par le nom du compartiment.
     - Dans ce cas, `StringNotEquals` remplacez *arn:aws:kms:region:111122223333:key/KMS* par le nom de ressource Amazon (ARN) à utiliser pour le KeyId chiffrement des résultats de votre découverte. AWS KMS key
   - Dans toutes les autres instructions, remplacez les valeurs d'espace réservé, où :
     - *myBucketName* est le nom du compartiment.
     - *111122223333* est l'identifiant de votre compte. Compte AWS
     - La *région* est Région AWS celle dans laquelle vous utilisez Macie et souhaitez autoriser Macie à ajouter les résultats de découverte au bucket.

       Si vous utilisez Macie dans plusieurs régions et que vous souhaitez autoriser Macie à ajouter des résultats au bucket pour des régions supplémentaires, ajoutez des `aws:SourceArn` conditions pour chaque région supplémentaire. Par exemple :

       ```
       "aws:SourceArn": [
           "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
       ```

```
    "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
    "arn:aws:macie2:us-west-2:111122223333:export-configuration:*",
    "arn:aws:macie2:us-west-2:111122223333:classification-job/*"
]
```

Vous pouvez également autoriser Macie à ajouter des résultats au bucket pour toutes les régions dans lesquelles vous utilisez Macie. Pour ce faire, remplacez la valeur de l'espace réservé par le caractère générique (*). Par exemple :

```
"aws:SourceArn": [
    "arn:aws:macie2:*:111122223333:export-configuration:*",
    "arn:aws:macie2:*:111122223333:classification-job/*"
]
```

- Si vous utilisez Macie dans une région optionnelle, ajoutez le code de région approprié à la valeur du `Service` champ de chaque instruction qui spécifie le principal du service Macie. Par exemple, si vous utilisez Macie dans la région du Moyen-Orient (Bahreïn), dont le code de région est me-south-1, `macie.amazonaws.com` remplacez-le par `macie.me-south-1.amazonaws.com` dans chaque énoncé applicable. Pour obtenir la liste des régions dans lesquelles Macie est actuellement disponible et le code régional de chacune d'entre elles, consultez la section Points de terminaison et quotas Amazon Macie dans le. Références générales AWS

Notez que l'exemple de politique inclut des instructions qui permettent à Macie de déterminer dans quelle région réside le compartiment (`GetBucketLocation`) et d'ajouter des objets au compartiment (`PutObject`). Ces instructions définissent les conditions qui utilisent deux clés de condition globales IAM :

- aws : SourceAccount — Cette condition permet à Macie d'ajouter les résultats de découverte de données sensibles au bucket uniquement pour votre compte. Cela empêche Macie d'ajouter les résultats de découverte d'autres comptes au bucket. Plus précisément, la condition indique quel compte peut utiliser le bucket pour les ressources et les actions spécifiées par la `aws:SourceArn` condition.

  Pour stocker les résultats de comptes supplémentaires dans le compartiment, ajoutez l'ID de compte de chaque compte supplémentaire à cette condition. Par exemple :

```
"aws:SourceAccount": [111122223333,444455556666]
```

- aws : SourceArn — Cette condition restreint l'accès au compartiment en fonction de la source des objets ajoutés au compartiment. Cela empêche les autres Services AWS utilisateurs d'ajouter des objets au compartiment. Cela empêche également Macie d'ajouter des objets au compartiment tout en effectuant d'autres actions pour votre compte. Plus précisément, cette condition permet à Macie d'ajouter des objets au compartiment uniquement si : les objets sont des résultats de découverte de données sensibles, et les résultats concernent la découverte automatique de données sensibles ou des tâches de découverte de données sensibles créées par le compte spécifié dans la région spécifiée.

  Pour permettre à Macie d'effectuer les actions spécifiées pour des comptes supplémentaires, ajoutez des ARN pour chaque compte supplémentaire à cette condition. Par exemple :

```
"aws:SourceArn": [
    "arn:aws:macie2:us-east-1:111122223333:export-configuration:*",
    "arn:aws:macie2:us-east-1:111122223333:classification-job/*",
    "arn:aws:macie2:us-east-1:444455556666:export-configuration:*",
    "arn:aws:macie2:us-east-1:444455556666:classification-job/*"
]
```

  Les comptes spécifiés par les `aws:SourceArn` conditions `aws:SourceAccount` et doivent correspondre.

  Ces deux conditions permettent d'éviter que Macie ne soit utilisée comme une adjointe confuse lors des transactions avec Amazon S3. Bien que cela ne soit pas recommandé, vous pouvez supprimer ces conditions de la politique relative aux compartiments.

8. Lorsque vous avez terminé de mettre à jour la politique de compartiment, choisissez Enregistrer les modifications.

Vous pouvez désormais configurer les paramètres du référentiel dans Macie.

Pour configurer les paramètres du référentiel dans Macie

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, sous Paramètres, sélectionnez Résultats de découverte.
3. Sous Référentiel pour les résultats de découverte de données sensibles, sélectionnez Compartiment existant.

4. Pour Choisir un compartiment, sélectionnez le compartiment dans lequel vous souhaitez stocker les résultats de votre découverte.
5. (Facultatif) Pour spécifier un préfixe à utiliser dans le chemin d'accès à un emplacement dans le compartiment, développez la section Avancé. Ensuite, pour le préfixe du résultat de la découverte des données, entrez le préfixe à utiliser.

   Lorsque vous entrez une valeur, Macie met à jour l'exemple ci-dessous pour indiquer le chemin d'accès à l'emplacement du compartiment où il stockera les résultats de votre découverte.
6. Sous Paramètres de chiffrement, spécifiez celui AWS KMS key que vous souhaitez que Macie utilise pour chiffrer les résultats :

   - Pour utiliser une clé de votre propre compte, choisissez Sélectionner une clé de votre compte. Ensuite, dans la AWS KMS keyliste, choisissez la clé à utiliser. La liste affiche les clés KMS de chiffrement symétriques gérées par le client pour votre compte.
   - Pour utiliser une clé détenue par un autre compte, choisissez Enter the ARN of a key from another account. Ensuite, dans le champ AWS KMS key ARN, entrez l'ARN de la clé à utiliser, par exemple. **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**
7. Lorsque vous avez fini de saisir les paramètres, choisissez Enregistrer.

   Macie teste les paramètres pour vérifier qu'ils sont corrects. Si certains paramètres sont incorrects, Macie affiche un message d'erreur pour vous aider à résoudre le problème.

Après avoir enregistré les paramètres du référentiel, Macie ajoute au référentiel les résultats de découverte existants des 90 jours précédents. Macie commence également à ajouter de nouveaux résultats de découverte au référentiel.

> **Note**
>
> Si vous modifiez par la suite le paramètre du préfixe des résultats de découverte des données, mettez également à jour la politique de compartiment dans Amazon S3. Les déclarations de politique qui spécifient le chemin précédent doivent spécifier le nouveau chemin. Sinon, Macie ne sera pas autorisé à ajouter les résultats de votre découverte au bucket.

> **Tip**
>
> Pour réduire les coûts de chiffrement côté serveur, configurez également le compartiment S3 pour utiliser une clé de compartiment S3 et spécifiez AWS KMS key celle que vous avez configurée pour le chiffrement des résultats de découverte de vos données sensibles. L'utilisation d'une clé de compartiment S3 permet de réduire le nombre d'appels AWS KMS, ce qui peut réduire les coûts liés aux AWS KMS demandes. Si la clé KMS se trouve dans un magasin de clés externe, l'utilisation d'une clé de compartiment S3 peut également minimiser l'impact sur les performances de l'utilisation de la clé. Pour en savoir plus, consultez la section Réduire le coût du SSE-KMS avec les clés de compartiment Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Classes et formats de stockage pris en charge par Amazon Macie

Pour vous aider à découvrir des données sensibles dans votre patrimoine de données Amazon Simple Storage Service (Amazon S3), Amazon Macie prend en charge la plupart des classes de stockage Amazon S3 et un large éventail de formats de fichiers et de stockage. Cette prise en charge s'applique à l'utilisation d'identifiants de données gérés et à l'utilisation d'identifiants de données personnalisés pour analyser les objets S3.

Pour que Macie puisse analyser un objet S3, celui-ci doit être stocké dans un compartiment Amazon S3 à usage général à l'aide d'une classe de stockage prise en charge. L'objet doit également utiliser un format de fichier ou de stockage compatible. Les rubriques de cette section répertorient les classes de stockage et les formats de fichiers et de stockage actuellement pris en charge par Macie.

> **Tip**
>
> Bien que Macie soit optimisé pour Amazon S3, vous pouvez l'utiliser pour découvrir des données sensibles dans des ressources que vous stockez actuellement ailleurs. Vous pouvez le faire en déplaçant les données vers Amazon S3 de manière temporaire ou permanente. Par exemple, exportez des instantanés Amazon Relational Database Service ou Amazon Aurora vers Amazon S3 au format Apache Parquet. Ou exportez une table Amazon DynamoDB vers Amazon S3. Vous pouvez ensuite créer une tâche de découverte de données sensibles pour analyser les données dans Amazon S3.

Rubriques

Classes de stockage Amazon S3 prises en charge

Pour la découverte de données sensibles, Amazon Macie prend en charge les classes de stockage Amazon S3 suivantes :

- Redondance réduite (RRS)
- S3 Glacier Instant Retrieval
- Hiérarchisation intelligente S3
- Accès peu fréquent à S3 One Zone (S3 One Zone-IA)
- S3 Standard
- Accès standard et peu fréquent (S3 Standard-IA)

Macie n'analyse pas les objets S3 qui utilisent d'autres classes de stockage Amazon S3, telles que S3 Glacier Deep Archive ou S3 Express One Zone. De plus, Macie n'analyse pas les objets stockés dans des compartiments de répertoire S3.

Si vous configurez une tâche de découverte de données sensibles pour analyser des objets S3 qui n'utilisent pas une classe de stockage Amazon S3 prise en charge, Macie ignore ces objets lors de l'exécution de la tâche. Macie n'essaie pas de récupérer ou d'analyser les données contenues dans les objets : les objets sont traités comme des objets inclassables. Un objet inclassable est un objet qui n'utilise aucune classe de stockage prise en charge ni aucun format de fichier ou de stockage pris en charge. Macie analyse uniquement les objets qui utilisent une classe de stockage et un format de fichier ou de stockage pris en charge.

De même, si vous configurez Macie pour effectuer la découverte automatique de données sensibles, les objets inclassables ne sont pas éligibles à la sélection et à l'analyse. Macie sélectionne uniquement les objets qui utilisent une classe de stockage Amazon S3 et un format de fichier ou de stockage pris en charge.

Pour identifier les compartiments S3 qui stockent des objets inclassables, vous pouvez filtrer votre inventaire de compartiments S3. Pour chaque compartiment de votre inventaire, des champs indiquent le nombre et la taille de stockage totale des objets inclassables qu'il contient.

Pour obtenir des informations détaillées sur les classes de stockage fournies par Amazon S3, consultez la section Utilisation des classes de stockage Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Formats de fichiers et de stockage pris en charge

Lorsqu'Amazon Macie analyse un objet S3, Macie extrait la dernière version de l'objet auprès d'Amazon S3, puis effectue une inspection approfondie du contenu de l'objet. Cette inspection prend en compte le format de fichier ou de stockage des données. Macie peut analyser des données dans de nombreux formats différents, y compris les formats de compression et d'archivage couramment utilisés.

Lorsque Macie analyse les données d'un fichier compressé ou d'archive, Macie inspecte à la fois le fichier complet et son contenu. Pour inspecter le contenu du fichier, Macie décompresse le fichier, puis inspecte chaque fichier extrait utilisant un format pris en charge. Macie peut le faire pour jusqu'à 1 000 000 de fichiers et jusqu'à une profondeur imbriquée de 10 niveaux. Pour plus d'informations sur les quotas supplémentaires applicables à la découverte de données sensibles, consultezQuotas Amazon Macie.

Le tableau suivant répertorie et décrit les types de fichiers et de formats de stockage que Macie peut analyser pour détecter les données sensibles. Pour chaque type pris en charge, le tableau répertorie également les extensions de nom de fichier applicables.

Type de fichier ou de stockage	Description	Extensions de nom de fichier
Big Data	Conteneurs d'objets Apache Avro et fichiers Apache Parquet	.avro, .parquet
Compression ou archivage	Archives compressées GNU Zip, archives TAR et archives compressées ZIP	.gz, .gzip, .tar, .zip
Document	Fichiers Adobe Portable Document Format, classeurs Microsoft Excel et documents Microsoft Word	.doc, .docx, .pdf, .xls, .xlsx

Type de fichier ou de stockage	Description	Extensions de nom de fichier
Message électronique	Fichiers de courrier électronique dont le contenu est conforme aux exigences spécifiées par une RFC de l'IETF pour les messages électroniques, telle que la RFC 2822	.eml
Texte	Fichiers texte non binaires tels que les fichiers CSV (valeurs séparées par des virgules), les fichiers HTML (Hypertext Markup Language), les fichiers JSON (JavaScript Object Notation), les fichiers JSON Lines, les documents en texte brut, les fichiers de valeurs séparées par des tabulations (TSV) et les fichiers XML (Extensible Markup Language)	.csv, .htm, .html, .json, .jsonl, .tsv, .txt, . et autres (selon le type de fichier texte non binaire)

Macie n'analyse pas les données contenues dans les images, le contenu audio, vidéo ou autre type de contenu multimédia.

Si vous configurez une tâche de découverte de données sensibles pour analyser des objets S3 qui n'utilisent aucun format de fichier ou de stockage pris en charge, Macie ignore ces objets lors de l'exécution de la tâche. Macie n'essaie pas de récupérer ou d'analyser les données contenues dans les objets : les objets sont traités comme des objets inclassables. Un objet inclassable est un objet qui n'utilise pas une classe de stockage Amazon S3 prise en charge ou un format de fichier ou de stockage pris en charge. Macie analyse uniquement les objets qui utilisent une classe de stockage et un format de fichier ou de stockage pris en charge.

De même, si vous configurez Macie pour effectuer la découverte automatique de données sensibles, les objets inclassables ne sont pas éligibles à la sélection et à l'analyse. Macie sélectionne

uniquement les objets qui utilisent une classe de stockage Amazon S3 et un format de fichier ou de stockage pris en charge.

Pour identifier les compartiments S3 qui stockent des objets inclassables, vous pouvez filtrer votre inventaire de compartiments S3. Pour chaque compartiment de votre inventaire, des champs indiquent le nombre et la taille de stockage totale des objets inclassables qu'il contient.

Analyse des résultats d'Amazon Macie

Amazon Macie génère des résultats lorsqu'il détecte des violations potentielles des politiques ou des problèmes liés à la sécurité ou à la confidentialité de vos compartiments à usage général Amazon Simple Storage Service (Amazon S3) ou lorsqu'il détecte des données sensibles dans des objets S3. Une constatation est un rapport détaillé d'un problème potentiel ou de données sensibles découvertes par Macie. Chaque découverte fournit une note de gravité, des informations sur la ressource affectée et des détails supplémentaires, tels que le moment et la manière dont Macie a découvert le problème ou les données. Macie conserve les informations relatives à vos politiques et à vos données sensibles pendant 90 jours.

Vous pouvez consulter, analyser et gérer les résultats des manières suivantes.

Console Amazon Macie

Les pages de résultats de la console Amazon Macie répertorient vos résultats et fournissent des informations détaillées sur les résultats individuels. Ces pages proposent également des options pour regrouper, filtrer et trier les résultats, ainsi que pour créer et gérer des règles de suppression. Les règles de suppression peuvent vous aider à rationaliser votre analyse des résultats.

API Amazon Macie

Avec l'API Amazon Macie, vous pouvez interroger et récupérer les données de résultats à l'aide d'un outil de ligne de AWS commande ou d'un AWS SDK, ou en envoyant des requêtes HTTPS directement à Macie. Pour interroger les données, vous soumettez une demande à l'API Amazon Macie et vous utilisez les paramètres pris en charge pour spécifier les résultats que vous souhaitez récupérer. Après avoir soumis votre demande, Macie renvoie les résultats dans une réponse JSON. Vous pouvez ensuite transmettre les résultats à un autre service ou une autre application pour une analyse plus approfondie ou à des fins de stockage ou de génération de rapports. Pour plus d'informations, consultez le manuel Amazon Macie API Reference.

Amazon EventBridge

Pour renforcer l'intégration avec d'autres services et systèmes, tels que les systèmes de surveillance ou de gestion des événements, Macie publie les résultats sur Amazon EventBridge sous forme d'événements. EventBridge, anciennement Amazon CloudWatch Events, est un service de bus d'événements sans serveur capable de fournir un flux de données en temps réel à partir de vos propres applications, d'applications logicielles en tant que service (SaaS), Services AWS telles que Macie. Il peut acheminer ces données vers des cibles telles que AWS Lambda

les fonctions, les rubriques Amazon Simple Notification Service et les flux Amazon Kinesis pour un traitement automatisé supplémentaire. L'utilisation de permet EventBridge également de garantir la conservation à long terme des données de résultats. Pour en savoir plus EventBridge, consultez le guide de EventBridge l'utilisateur Amazon.

Macie publie automatiquement des événements EventBridge pour obtenir de nouvelles découvertes. Il publie également des événements automatiquement pour les occurrences ultérieures de conclusions politiques existantes. Les données des résultats étant structurées sous forme d' EventBridge événements, vous pouvez plus facilement surveiller, analyser et agir en fonction des résultats en utilisant d'autres services et outils. Par exemple, vous pouvez l'utiliser EventBridge pour envoyer automatiquement des types spécifiques de nouvelles découvertes à une AWS Lambda fonction qui, à son tour, traite et envoie les données à votre système de gestion des incidents et événements de sécurité (SIEM). Si vous intégrez les notifications utilisateur AWS à Macie, vous pouvez également utiliser les événements pour être automatiquement informé des résultats via les canaux de diffusion que vous spécifiez. Pour en savoir plus sur l'utilisation EventBridge des événements pour surveiller et traiter les résultats, voirIntégration d'Amazon Macie à Amazon EventBridge.

AWS Security Hub

Pour une analyse plus approfondie du niveau de sécurité de votre entreprise, vous pouvez également publier les résultats sur AWS Security Hub. Security Hub est un service qui collecte des données de sécurité à partir Services AWS des solutions de AWS Partner Network sécurité prises en charge afin de vous fournir une vue complète de l'état de sécurité de votre AWS environnement. Security Hub vous permet également de vérifier que votre environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité. Pour en savoir plus sur Security Hub, consultez le guide de AWS Security Hub l'utilisateur. Pour en savoir plus sur l'utilisation de Security Hub pour surveiller et traiter les résultats, consultezIntégration d'Amazon Macie avec AWS Security Hub.

Outre les résultats, Macie crée des résultats de découverte de données sensibles pour les objets S3 qu'il analyse pour découvrir des données sensibles. Un résultat de découverte de données sensibles est un enregistrement qui consigne les détails de l'analyse d'un objet. Cela inclut les objets dans lesquels Macie ne trouve pas de données sensibles et ne produit donc pas de résultats, ainsi que les objets que Macie ne peut pas analyser en raison d'erreurs ou de problèmes. Les résultats de découverte de données sensibles vous fournissent des enregistrements d'analyse qui peuvent être utiles pour les audits ou les enquêtes sur la confidentialité et la protection des données. Vous ne pouvez pas accéder aux résultats de découverte de données sensibles directement sur la console

Amazon Macie ou via l'API Amazon Macie. Au lieu de cela, vous configurez Macie pour stocker les résultats dans un compartiment S3. Vous pouvez ensuite éventuellement accéder aux résultats contenus dans ce compartiment et les interroger. Pour savoir comment configurer Macie pour stocker les résultats, consultezStockage et conservation des résultats de découverte de données sensibles.

Rubriques

Types de résultats sur Amazon Macie

Amazon Macie génère deux catégories de résultats : les résultats relatifs aux politiques et les résultats relatifs aux données sensibles. Une constatation de politique est un rapport détaillé faisant état d'une violation potentielle d'une politique ou d'un problème lié à la sécurité ou à la confidentialité d'un bucket à usage général Amazon Simple Storage Service (Amazon S3). Macie produit des conclusions relatives aux politiques dans le cadre de ses activités continues visant à évaluer et à surveiller vos compartiments à usage général en matière de sécurité et de contrôle d'accès. Une découverte de données sensibles est un rapport détaillé des données sensibles détectées par Macie dans un objet S3. Macie génère des découvertes de données sensibles dans le cadre des activités qu'il effectue lorsque vous exécutez des tâches de découverte de données sensibles ou lorsqu'il effectue une découverte automatique de données sensibles.

Dans chaque catégorie, il existe des types spécifiques. Le type de résultat donne un aperçu de la nature du problème ou des données sensibles détectées par Macie. Les détails d'une constatation fournissent une note de gravité, des informations sur la ressource affectée et des informations supplémentaires, telles que le moment et la manière dont Macie a découvert le problème ou des données sensibles. La gravité et les détails de chaque constatation varient en fonction du type et de la nature de la constatation.

Rubriques

- Types de conclusions relatives aux politiques
- Types de résultats relatifs à des données sensibles

> **Tip**
>
> Pour explorer et découvrir les différentes catégories et types de résultats que Macie peut générer, créez des exemples de résultats. Les exemples de résultats utilisent des exemples de données et des valeurs d'espace réservé pour démontrer le type d'informations que chaque type de résultat peut contenir.

Types de conclusions relatives aux politiques

Amazon Macie génère une recherche de politique lorsque les politiques ou les paramètres d'un compartiment à usage général S3 sont modifiés d'une manière qui réduit la sécurité ou la confidentialité du compartiment et de ses objets. Pour plus d'informations sur la façon dont Macie détecte ces modifications, consultezComment Macie surveille la sécurité des données Amazon S3.

Macie génère une recherche de politique uniquement si le changement intervient après que vous avez activé Macie pour votre. Compte AWS Par exemple, si les paramètres de blocage de l'accès public sont désactivés pour un compartiment S3 après avoir activé Macie, Macie génère une recherche BlockPublicAccessDisabledPolicy:IAMuser/S3 pour le compartiment. Si les paramètres de blocage de l'accès public étaient désactivés pour un bucket lorsque vous avez activé Macie et qu'ils continuent de l'être, Macie ne génère pas de recherche BlockPublicAccessDisabledPolicy:IAMuser/S3 pour le bucket.

Si Macie détecte une occurrence ultérieure d'une constatation de politique existante, Macie met à jour la constatation existante en ajoutant des détails sur l'occurrence suivante et en augmentant le nombre d'occurrences. Macie conserve les résultats de ses politiques pendant 90 jours.

Macie peut générer les types de conclusions politiques suivants pour un bucket S3 à usage général.

Policy:IAMUser/S3BlockPublicAccessDisabled

Tous les paramètres de blocage de l'accès public au niveau du compartiment ont été désactivés pour le compartiment. L'accès au bucket est contrôlé par les paramètres de blocage de l'accès public pour le compte, les listes de contrôle d'accès (ACL) et la politique du bucket pour le bucket.

Pour en savoir plus sur les paramètres de blocage de l'accès public pour les compartiments S3, consultez la section Blocage de l'accès public à votre espace de stockage Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Policy:IAMUser/S3BucketEncryptionDisabled

Les paramètres de chiffrement par défaut du compartiment ont été réinitialisés selon le comportement de chiffrement par défaut d'Amazon S3, qui consiste à chiffrer automatiquement les nouveaux objets avec une clé gérée par Amazon S3.

À compter du 5 janvier 2023, Amazon S3 applique automatiquement le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de chiffrement de base pour les objets ajoutés aux compartiments. Vous pouvez éventuellement configurer les paramètres de chiffrement par défaut d'un compartiment pour utiliser à la place le chiffrement côté serveur avec une AWS KMS clé (SSE-KMS) ou le chiffrement double couche côté serveur avec une clé (DSSE-KMS). AWS KMS Pour en savoir plus sur les paramètres et options de chiffrement par défaut pour les compartiments S3, consultez la section Définition du comportement de chiffrement côté serveur par défaut pour les compartiments S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Si Macie a généré ce type de découverte avant le 5 janvier 2023, cela indique que les paramètres de chiffrement par défaut ont été désactivés pour le compartiment concerné. Cela signifiait que les paramètres du compartiment ne spécifiaient pas le comportement de chiffrement par défaut côté serveur pour les nouveaux objets. La possibilité de désactiver les paramètres de chiffrement par défaut pour un compartiment n'est plus prise en charge par Amazon S3.

Policy:IAMUser/S3BucketPublic

Une politique d'ACL ou de compartiment pour le compartiment a été modifiée pour autoriser l'accès aux utilisateurs anonymes ou à toutes les identités authentifiées AWS Identity and Access Management (IAM).

Pour en savoir plus sur les ACL et les politiques de compartiment pour les compartiments S3, consultez la section Gestion des identités et des accès dans Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Policy:IAMUser/S3BucketReplicatedExternally

La réplication a été activée et configurée pour répliquer des objets du compartiment vers un compartiment externe à votre organisation (ne faisant pas partie de celui-ci). Compte AWS Une organisation est un ensemble de comptes Macie gérés de manière centralisée en tant que groupe de comptes connexes via AWS Organizations ou sur invitation de Macie.

Dans certaines conditions, Macie peut générer ce type de recherche pour un bucket qui n'est pas configuré pour répliquer des objets vers un bucket externe. Compte AWS Cela peut se produire si le compartiment de destination a été créé différemment Région AWS au cours des 24 heures précédentes, après que Macie ait récupéré les métadonnées du bucket et de l'objet sur Amazon S3 dans le cadre du cycle d'actualisation quotidien. Pour étudier le résultat, commencez par actualiser les données de votre inventaire. Passez ensuite en revue les détails du compartiment. Les détails indiquent si le compartiment est configuré pour répliquer des objets dans d'autres compartiments. Si le bucket est configuré pour cela, les détails incluent l'ID de compte pour chaque compte propriétaire d'un bucket de destination.

Pour en savoir plus sur les paramètres de réplication pour les compartiments S3, consultez la section Réplication d'objets dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Policy:IAMUser/S3BucketSharedExternally

Une ACL ou une politique de bucket pour le bucket a été modifiée afin de permettre le partage du bucket avec une Compte AWS personne externe (ne faisant pas partie) de votre organisation. Une organisation est un ensemble de comptes Macie gérés de manière centralisée en tant que groupe de comptes connexes via AWS Organizations ou sur invitation de Macie.

Dans certains cas, Macie peut générer ce type de recherche pour un compartiment qui n'est pas partagé avec un compte AWS externe. Cela peut se produire si Macie n'est pas en mesure d'évaluer pleinement la relation entre l'`Principal`élément de la politique du compartiment et certaines clés de contexte de condition AWS globales ou les clés de condition Amazon S3 présentes dans l'`Condition`élément de la politique. Les clés de condition applicables sont les suivantes : `aws:PrincipalAccount` `aws:PrincipalArn` `aws:PrincipalOrgID` `aws:PrincipalOrgPaths`, `aws:PrincipalTag`, `aws:PrincipalType`, `aws:ets3:DataAccessPointArn`. Nous vous recommandons de consulter la politique du bucket afin de déterminer si cet accès est prévu et sûr.

Pour en savoir plus sur les ACL et les politiques de compartiment pour les compartiments S3, consultez la section Gestion des identités et des accès dans Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Policy:IAMUser/S3BucketSharedWithCloudFront

La politique relative au compartiment a été modifiée pour permettre le partage du compartiment avec une identité d'accès à l' CloudFront origine (OAI) Amazon, un contrôle CloudFront d'accès à l'origine (OAC), ou à la fois avec un CloudFront OAI et un OAC. CloudFront Un CloudFront

OAI ou un OAC permet aux utilisateurs d'accéder aux objets d'un bucket via une ou plusieurs distributions spécifiées CloudFront.

Pour en savoir plus sur les CloudFront OAI et les OAC, consultez Restreindre l'accès à une origine Amazon S3 dans le manuel Amazon CloudFront Developer Guide.

> **Note**
>
> Dans certains cas, Macie génère une recherche Policy:IAMuser/S3 au lieu d'une BucketSharedExternally recherche Policy:IAMuser/S3 pour un bucket. BucketSharedWithCloudFront Ces cas sont les suivants :
>
> - Le bucket est partagé avec un tiers Compte AWS externe à votre organisation, en plus d'un CloudFront OAI ou d'un OAC.
> - La politique du bucket spécifie un ID utilisateur canonique, au lieu de l'Amazon Resource Name (ARN), d'un CloudFront OAI.
>
> Cela permet de trouver une politique de sévérité plus élevée pour le compartiment.

Types de résultats relatifs à des données sensibles

Macie génère une recherche de données sensibles lorsqu'il détecte des données sensibles dans un objet S3 qu'il analyse pour découvrir des données sensibles. Cela inclut les analyses effectuées par Macie lorsque vous exécutez une tâche de découverte de données sensibles ou lorsqu'il effectue une découverte automatique de données sensibles.

Par exemple, si vous créez et exécutez une tâche de découverte de données sensibles et que Macie détecte des numéros de compte bancaire dans un objet S3, Macie génère un résultat SensitiveData :S3Object/Financial finding pour l'objet. De même, si Macie détecte des numéros de compte bancaire dans un objet S3 qu'il analyse au cours d'un cycle automatique de découverte de données sensibles, Macie génère un résultat SensitiveData :S3Object/Financial pour l'objet.

Si Macie détecte des données sensibles dans le même objet S3 lors d'une exécution de tâche ultérieure ou d'un cycle de découverte automatique de données sensibles, Macie génère une nouvelle recherche de données sensibles pour l'objet. Contrairement aux conclusions relatives aux politiques, toutes les découvertes relatives aux données sensibles sont traitées comme nouvelles (uniques). Macie conserve les résultats de données sensibles pendant 90 jours.

Macie peut générer les types suivants de résultats de données sensibles pour un objet S3.

SensitiveData:S3Object/Credentials

L'objet contient des données d'identification sensibles, telles que des clés d'accès AWS secrètes ou des clés privées.

SensitiveData:S3Object/CustomIdentifier

L'objet contient du texte qui correspond aux critères de détection d'un ou de plusieurs identificateurs de données personnalisés. L'objet peut contenir plusieurs types de données sensibles.

SensitiveData:S3Object/Financial

L'objet contient des informations financières sensibles, telles que des numéros de compte bancaire ou de carte de crédit.

SensitiveData:S3Object/Multiple

L'objet contient plusieurs catégories de données sensibles : toute combinaison de données d'identification, d'informations financières, d'informations personnelles ou de texte correspondant aux critères de détection d'un ou de plusieurs identifiants de données personnalisés.

SensitiveData:S3Object/Personal

L'objet contient des informations personnelles sensibles : des informations personnelles identifiables (PII) telles que les numéros de passeport ou de permis de conduire, des informations médicales personnelles (PHI) telles que les numéros d'assurance maladie ou d'identification médicale, ou une combinaison de PII et PHI.

Pour plus d'informations sur les types de données sensibles que Macie peut détecter à l'aide de critères et de techniques intégrés, consultezUtilisation des identificateurs de données gérés. Pour plus d'informations sur les types d'objets S3 que Macie peut analyser, consultezClasses et formats de stockage pris en charge.

Utilisation des résultats d'échantillons dans Amazon Macie

Pour découvrir et découvrir les différents types de résultats qu'Amazon Macie peut générer, vous pouvez créer des exemples de résultats. Les exemples de résultats utilisent des exemples de données et des valeurs d'espace réservé pour démontrer le type d'informations que chaque type de résultat peut contenir.

Par exemple, l'BucketPublicexemple de recherche Policy:IAMuser/S3 contient des informations sur un bucket Amazon Simple Storage Service (Amazon S3) fictif. Les détails du résultat incluent des exemples de données concernant un acteur et une action qui ont modifié la liste de contrôle d'accès (ACL) du bucket et l'ont rendu accessible au public. De même, la recherche:S3Object/Multiple SensitiveDataSample contient des détails sur un classeur Microsoft Excel fictif. Les détails du résultat incluent des exemples de données concernant les types et l'emplacement des données sensibles dans le classeur.

En plus de vous familiariser avec les informations que peuvent contenir différents types de résultats, vous pouvez utiliser des exemples de résultats pour tester l'intégration avec d'autres applications, services et systèmes. Selon les règles de suppression de votre compte, Macie peut publier des exemples de résultats sur Amazon EventBridge sous forme d'événements. En utilisant les données d'exemple dans les résultats d'échantillonnage, vous pouvez développer et tester des solutions automatisées pour surveiller et traiter ces événements. En fonction des paramètres de publication de votre compte, Macie peut également publier des exemples de résultats sur. AWS Security Hub Cela signifie que vous pouvez également utiliser des exemples de résultats pour développer et tester des solutions de surveillance et de traitement des résultats Macie dans Security Hub. Pour plus d'informations sur la publication des résultats vers ces services, consultezSurveillance et traitement des résultats.

Rubriques

- Création d'échantillons de résultats
- Examen des résultats d'un échantillon
- Suppression des résultats des échantillons

Création d'échantillons de résultats

Vous pouvez créer des exemples de résultats à l'aide de la console Amazon Macie ou de l'API Amazon Macie. Si vous utilisez la console, Macie génère automatiquement un échantillon de recherche pour chaque type de recherche pris en charge par Macie. Si vous utilisez l'API, vous pouvez créer un échantillon pour chaque type ou uniquement pour certains types que vous spécifiez.

Console

Suivez ces étapes pour créer des exemples de résultats à l'aide de la console Amazon Macie.

Pour créer des exemples de résultats

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sous Exemples de résultats, choisissez Générer des exemples de résultats.

API

Pour créer des exemples de résultats par programmation, utilisez le CreateSampleFindingsfonctionnement de l'API Amazon Macie. Lorsque vous soumettez votre demande, utilisez éventuellement le `findingTypes` paramètre pour spécifier uniquement certains types d'échantillons de résultats à créer. Pour créer automatiquement des échantillons de tous types, n'incluez pas ce paramètre dans votre demande.

Pour créer des exemples de résultats à l'aide de AWS Command Line Interface(AWS CLI), exécutez la create-sample-findingscommande. Pour créer automatiquement des échantillons de tous les types de résultats, n'incluez pas le `finding-types` paramètre. Pour créer des échantillons de certains types de résultats uniquement, incluez ce paramètre et spécifiez les types d'échantillons de résultats à créer. Par exemple :

```
C:\> aws macie2 create-sample-findings --finding-types "SensitiveData:S3Object/
Multiple" "Policy:IAMUser/S3BucketPublic"
```

Where:S3Object/Multiple SensitiveDataest un type de recherche de données sensibles à créer et Policy:IAMuser/S3 est un type de recherche de politique à créer. BucketPublic

Si la commande s'exécute correctement, Macie renvoie une réponse vide.

Examen des résultats d'un échantillon

Pour vous aider à identifier les résultats d'échantillonnage que vous avez créés, Macie définit la valeur du champ Échantillon de chaque résultat d'échantillon sur True. En outre, le nom du compartiment S3 concerné est le même pour tous les résultats de l'échantillon : macie-sample-finding-bucket. Si vous consultez les résultats d'un échantillon à l'aide des pages Résultats de la console Amazon Macie, Macie affiche également le préfixe [SAMPLE] dans le champ Type de recherche pour chaque résultat d'échantillon.

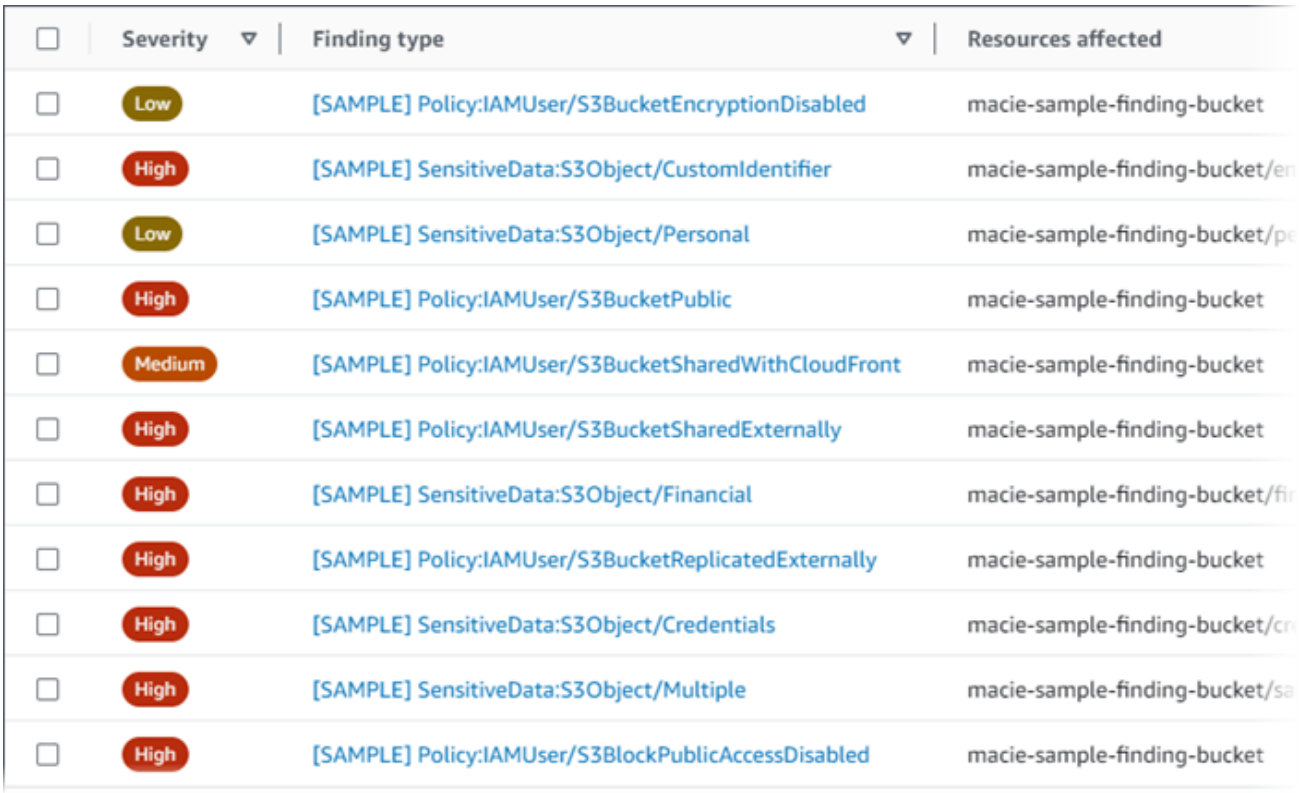
Console

Suivez ces étapes pour consulter les exemples de résultats à l'aide de la console Amazon Macie.

Pour examiner les résultats d'un échantillon

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Conclusions.
3. Sur la page Résultats, effectuez l'une des opérations suivantes :

   - Dans la colonne Type de recherche, localisez les résultats dont le type commence par [SAMPLE], comme indiqué dans l'image suivante.



   - À l'aide de la zone Critères de filtrage située au-dessus du tableau, filtrez le tableau pour n'afficher que des échantillons de résultats. Pour ce faire, placez votre curseur dans la case. Dans la liste des champs qui s'affiche, choisissez Sample. Choisissez ensuite Vrai, puis Appliquer. Cela ajoute la condition de filtre suivante au tableau :

4. Pour consulter les détails d'un résultat d'échantillonnage spécifique, choisissez le résultat. Le panneau des détails affiche des informations relatives au résultat.

Vous pouvez également télécharger et enregistrer les détails d'un ou de plusieurs exemples de résultats sous forme de fichier JSON. Pour ce faire, cochez la case correspondant à chaque exemple de résultat que vous souhaitez télécharger et enregistrer. Choisissez ensuite Exporter (JSON) dans le menu Actions en haut de la page des résultats. Dans la fenêtre qui s'affiche, choisissez Télécharger. Pour obtenir une description détaillée des champs JSON qu'une recherche peut inclure, consultez la section Conclusions du manuel Amazon Macie API Reference.

API

Pour examiner les résultats d'un échantillon par programmation, utilisez d'abord le ListFindingsfonctionnement de l'API Amazon Macie pour récupérer l'identifiant unique `findingId` () pour chaque échantillon de recherche que vous avez créé. Utilisez ensuite l'GetFindingsopération pour récupérer les détails de ces résultats.

Lorsque vous soumettez la ListFindings demande, vous pouvez définir des critères de filtre afin d'inclure uniquement les résultats des échantillons dans les résultats. Pour ce faire, ajoutez une condition de filtre dans laquelle la valeur du `sample` champ est`true`. Si vous utilisez leAWS CLI, exécutez la commande list-findings et utilisez le `finding-criteria` paramètre pour spécifier la condition du filtre. Par exemple :

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"sample\":{\"eq\":
[\"true\"]}}}
```

Si votre demande aboutit, Macie renvoie un `findingIds` tableau. Le tableau répertorie l'identifiant unique pour chaque échantillon trouvé pour votre compte dans le courantRégion AWS.

Pour récupérer ensuite les détails des exemples de résultats, spécifiez ces identifiants uniques dans une GetFindings demande ou, dans le cas duAWS CLI, lorsque vous exécutez la commande get-findings.

Suppression des résultats des échantillons

Comme les autres résultats, Macie conserve les résultats des échantillons pendant 90 jours. Une fois que vous avez terminé de réviser et d'expérimenter les échantillons, vous pouvez éventuellement les archiver en créant une règle de suppression. Dans ce cas, les résultats de l'échantillon ne s'affichent plus par défaut sur la console et leur statut devient archivé.

Pour archiver les résultats des échantillons à l'aide de la console Amazon Macie, configurez la règle pour archiver les résultats lorsque la valeur du champ Sample est True. Pour archiver des exemples de résultats à l'aide de l'API Amazon Macie, configurez la règle pour archiver les résultats où se trouve la valeur du `sample` champ. `true`

Examen des résultats sur la console Amazon Macie

Amazon Macie surveille votre AWS environnement et génère des informations relatives aux politiques lorsqu'il détecte des violations potentielles des politiques ou des problèmes liés à la sécurité ou à la confidentialité de vos compartiments à usage général Amazon Simple Storage Service (Amazon S3). Macie génère des résultats de données sensibles lorsqu'il détecte des données sensibles dans des objets S3. Macie conserve les informations relatives à vos politiques et à vos données sensibles pendant 90 jours.

Chaque constatation spécifie un type de constatation et un indice de gravité. Les détails supplémentaires incluent des informations sur la ressource affectée et sur le moment et la manière dont Macie a découvert le problème ou sur les données sensibles signalées par la découverte. La gravité et les détails de chaque constatation varient en fonction du type et de la nature de la constatation.

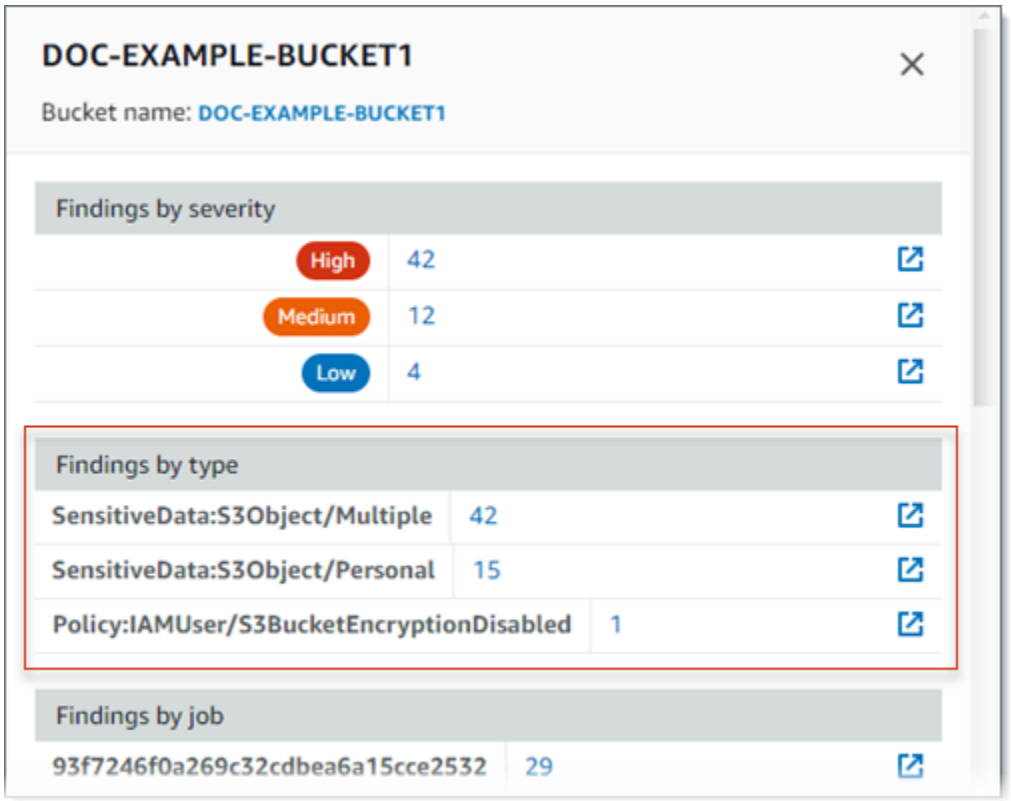
À l'aide de la console Amazon Macie, vous pouvez consulter et analyser les résultats, et accéder au détail des résultats individuels. Vous pouvez également exporter un ou plusieurs résultats vers un fichier JSON. Pour vous aider à rationaliser votre analyse, la console propose plusieurs options pour créer des vues personnalisées des résultats.

Utiliser des groupements prédéfinis

Utilisez des pages spécifiques pour examiner les résultats regroupés selon des critères tels que le compartiment S3 concerné, le type de recherche ou la tâche de découverte de données sensibles. Ces pages vous permettent de consulter les statistiques agrégées pour chaque groupe, telles que le nombre de résultats par gravité. Vous pouvez également effectuer une analyse détaillée des résultats individuels d'un groupe, et vous pouvez appliquer des filtres pour affiner votre analyse.

Par exemple, si vous regroupez tous les résultats par compartiment S3 et que vous remarquez qu'un compartiment particulier présente une violation des règles, vous pouvez rapidement déterminer s'il existe également des résultats de données sensibles pour le compartiment. Pour ce faire, choisissez Par compartiment dans le volet de navigation (sous Résultats), puis choisissez

le compartiment. Dans le panneau de détails qui apparaît, la section Résultats par type répertorie les types de résultats qui s'appliquent au bucket, comme illustré dans l'image suivante.

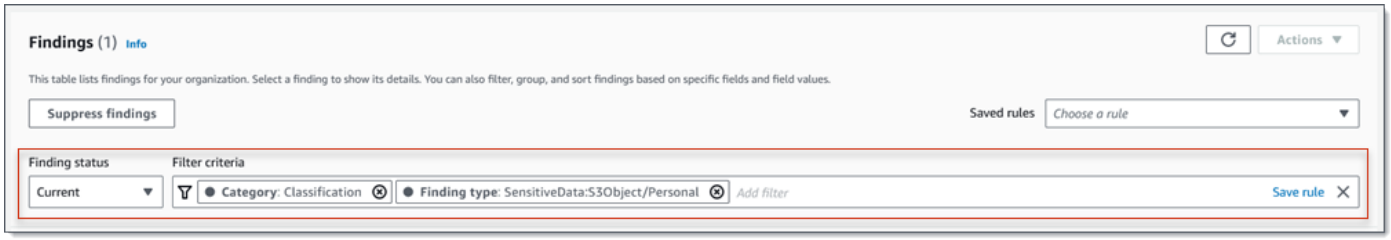


Pour étudier un type spécifique, choisissez le numéro du type. Macie affiche un tableau de tous les résultats correspondant au type sélectionné et s'appliquant au compartiment S3. Pour affiner les résultats, filtrez le tableau.

Création et application de filtres

Utilisez des attributs de recherche spécifiques pour inclure ou exclure certains résultats d'un tableau de résultats. Un attribut de recherche est un champ qui stocke des données spécifiques pour une recherche, telles que le type de recherche, la gravité ou le nom du compartiment S3 concerné. Si vous filtrez un tableau, vous pouvez identifier plus facilement les résultats présentant des caractéristiques spécifiques. Vous pouvez ensuite passer en revue les détails de ces résultats.

Par exemple, pour examiner toutes les données sensibles que vous avez trouvées, ajoutez des critères de filtre pour le champ Catégorie. Pour affiner les résultats et n'inclure qu'un type spécifique de recherche de données sensibles, ajoutez des critères de filtre pour le champ Type de recherche. Par exemple :



Pour passer ensuite en revue les détails d'une constatation particulière, choisissez-la. Le panneau des détails affiche des informations relatives au résultat.

Vous pouvez également trier les résultats par ordre croissant ou décroissant selon certains champs. Pour ce faire, choisissez l'en-tête de colonne du champ. Pour modifier l'ordre de tri, choisissez à nouveau l'en-tête de colonne.

Pour consulter les résultats sur la console

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Conclusions. La page Résultats affiche les résultats que Macie a créés ou mis à jour pour votre compte au Région AWS cours des 90 derniers jours. Par défaut, cela n'inclut pas les résultats supprimés par une règle de suppression.
3. Pour passer en revue les résultats d'un groupe logique prédéfini et les examiner, choisissez Par compartiment, Par type ou Par tâche dans le volet de navigation (sous Résultats). Choisissez ensuite un élément dans le tableau. Dans le panneau de détails, choisissez le lien vers lequel le champ doit être pivoté.
4. Pour filtrer les résultats selon des critères spécifiques, utilisez les options de filtrage situées au-dessus du tableau :

   - Pour afficher les résultats supprimés par une règle de suppression, utilisez le menu État de la recherche. Choisissez Tout pour afficher à la fois les résultats supprimés et non supprimés, ou choisissez Archivé pour afficher uniquement les résultats supprimés. Pour masquer à nouveau les résultats supprimés, choisissez Current.
   - Pour afficher uniquement les résultats dotés d'un attribut spécifique, utilisez la zone Critères de filtrage. Placez votre curseur dans le champ et ajoutez une condition de filtre pour l'attribut. Pour affiner davantage les résultats, ajoutez des conditions pour des attributs supplémentaires. Pour supprimer ensuite une condition, cliquez sur l'icône de suppression de la condition

( ) correspondant à la condition à supprimer.

Pour plus d'informations sur le filtrage des résultats, consultez Création et application de filtres aux résultats.

5. Pour trier les résultats par champ spécifique, choisissez l'en-tête de colonne correspondant au champ. Pour modifier l'ordre de tri, choisissez à nouveau l'en-tête de colonne.
6. Pour consulter les détails d'un résultat spécifique, choisissez-le. Le panneau des détails affiche des informations relatives au résultat.

> **Tip**
>
> Vous pouvez utiliser le panneau de détails pour pivoter et explorer certains champs vers le bas. Pour afficher les résultats qui ont la même valeur pour un champ, choisissez dans le champ. Vous pouvez également choisir d'afficher les résultats contenant d'autres valeurs pour le champ.
> Pour rechercher des données sensibles, vous pouvez également utiliser le panneau de détails pour examiner les données sensibles trouvées par Macie dans l'objet S3 concerné :
>
> - Pour localiser les occurrences d'un type spécifique de données sensibles, choisissez le lien numérique dans le champ correspondant à ce type de données. Macie affiche des informations (au format JSON) sur l'endroit où Macie a trouvé les données. Pour plus d'informations, consultez Find occurrences données sensibles sensibles sensibles.
> - Pour récupérer des échantillons des données sensibles trouvées par Macie, choisissez Revoir dans le champ Afficher les échantillons. Pour plus d'informations, consultez Récupération d'échantillons de données sensibles.
> - Pour accéder au résultat de découverte de données sensibles correspondant, cliquez sur le lien dans le champ Emplacement détaillé des résultats. Macie ouvre la console Amazon S3 et affiche le fichier ou le dossier contenant le résultat de la découverte. Pour plus d'informations, consultez Stockage et conservation des résultats de découverte de données sensibles.

Vous pouvez également télécharger et enregistrer les détails d'un ou de plusieurs résultats sous forme de fichier JSON. Pour ce faire, cochez la case correspondant à chaque recherche que vous souhaitez télécharger et enregistrer. Choisissez ensuite Exporter (JSON) dans le menu Actions en haut de la page des résultats. Dans la fenêtre qui s'affiche, choisissez Télécharger. Pour obtenir une description détaillée des champs JSON qu'une recherche peut inclure, consultez la section Conclusions du manuel Amazon Macie API Reference.

Filtrage Amazon Macie ie ie ie ie ie ie

Pour effectuer une analyse ciblée et analyser les résultats de manière plus efficace, vous pouvez filtrer les résultats d'Amazon Macie. Les filtres vous permettent de créer des vues et des requêtes personnalisées pour les résultats, ce qui peut vous aider à identifier et à vous concentrer sur les résultats qui ont des caractéristiques spécifiques. Utilisez la console Amazon Macie pour filtrer les résultats ou envoyez des requêtes de manière programmatique à l'aide de l'API Amazon Macie.

Lorsque vous créez un filtre, vous utilisez des attributs spécifiques des résultats pour définir des critères permettant d'inclure ou d'exclure des résultats d'une vue ou des résultats d'une requête. Un attribut de recherche est un champ qui stocke des données spécifiques pour une constatation, telles que la gravité, le type ou le nom du compartiment S3 auquel une constatation s'applique.

Dans Macie ie ie ie ie ie ie ie ie ie ie ie ie macie ie ie Macie ie ie ie ie ie Chaque condition, également appelée critère, se compose de trois parties :

- Un champ basé sur un attribut, tel que la gravité ou le type de recherche.
- Un opérateur, tel que égal ou non égal.
- Une ou plusieurs valeurs. Le type et le nombre de valeurs dépendent du champ et de l'opérateur que vous choisissez.

Si vous créez un filtre que vous souhaitez réutiliser, vous pouvez l'enregistrer en tant que règle de filtre. Une règle de filtrage est un ensemble de critères de filtre que vous créez et enregistrez pour les appliquer à nouveau lorsque vous consultez les résultats sur la console Amazon Macie.

Vous pouvez également enregistrer un filtre en tant que règle de suppression. Une règle de suppression est un ensemble de critères de filtre que vous créez et enregistrez pour archiver automatiquement les résultats qui correspondent aux critères de la règle. Pour en savoir plus sur les règles de suppression, consultezSuppression de résultats.

Rubriques

Principes fondamentaux du filtrage des résultats

Lorsque vous créez un filtre, tenez compte des fonctionnalités et directives suivantes. Notez également que les résultats filtrés sont limités aux 90 jours précédents et aux 90 jours actuelsRégion AWS. Amazon Macie ne conserve vos résultats que pendant 90 jours par recherche. Région AWS

Rubriques

Utilisation de plusieurs conditions dans un filtre

Un filtre peut inclure une ou plusieurs conditions. Chaque condition, également appelée critère, comprend trois parties :

- Champ basé sur un attribut, tel que la gravité ou le type de recherche. Pour obtenir la liste des champs que vous pouvez utiliser, consultezChamps pour filtrer les résultats.
- Un opérateur, tel que égal ou non égal. Pour obtenir la liste des opérateurs que vous pouvez utiliser, consultezUtilisation d'opérateurs dans des conditions.
- Une ou plusieurs valeurs. Le type et le nombre de valeurs dépendent du champ et de l'opérateur que vous choisissez.

Si un filtre contient plusieurs conditions, Macie utilise la logique AND pour joindre les conditions et évaluer les critères du filtre. Cela signifie qu'un résultat correspond aux critères du filtre uniquement s'il répond à toutes les conditions du filtre.

Par exemple, si vous ajoutez une condition pour inclure uniquement les résultats de gravité élevée et une autre condition pour inclure uniquement les résultats de données sensibles, Macie renvoie

tous les résultats de données sensibles de gravité élevée. En d'autres termes, Macie exclut tous les résultats relatifs aux politiques et tous les résultats de données sensibles de gravité moyenne ou faible.

Vous ne pouvez utiliser un champ qu'une seule fois dans un filtre. Vous pouvez toutefois spécifier plusieurs valeurs pour de nombreux champs.

Par exemple, si un état utilise le champ Sévérité pour inclure uniquement des résultats de gravité élevée, vous ne pouvez pas utiliser le champ Sévérité dans un autre état pour inclure des résultats de gravité moyenne ou faible. Spécifiez plutôt plusieurs valeurs pour la condition existante ou utilisez un opérateur différent pour la condition existante. Par exemple, pour inclure tous les résultats de gravité moyenne et élevée, ajoutez un état de gravité égal à moyen ou élevé ou ajoutez un état de gravité différent de faible.

Spécification de valeurs pour les champs

Lorsque vous spécifiez une valeur pour un champ, celle-ci doit être conforme au type de données sous-jacent du champ. En fonction du champ, vous pouvez spécifier l'un des types de valeurs suivants.

Tableau de texte (chaînes)

Spécifie une liste de valeurs de texte (chaîne) pour un champ. Chaque chaîne est corrélée à une valeur prédéfinie ou existante pour un champ, par exemple, High pour le champ Severity, :S3Object/Financial pour le champ de type Finding, ou le nom d'un compartiment S3 SensitiveDatapour le champ de nom du compartiment S3.

Si vous utilisez un tableau, notez ce qui suit :

- Les valeurs distinguent les majuscules et minuscules.
- Vous ne pouvez pas spécifier de valeurs partielles ni utiliser de caractères génériques dans les valeurs. Vous devez spécifier une valeur complète et valide pour le champ.

Par exemple, pour filtrer les résultats d'un compartiment S3 nommé My-S3-bucket, entrez **`my-S3-bucket`** la valeur du champ Nom du compartiment S3. Si vous entrez une autre valeur, telle que **`my-s3-bucket`** ou**`my-S3`**, Macie ne renverra pas les résultats pour le bucket.

Pour obtenir la liste des valeurs valides pour chaque champ, consultezChamps pour filtrer les résultats.

Vous pouvez spécifier jusqu'à 50 valeurs dans un tableau. La façon dont vous spécifiez les valeurs varie selon que vous utilisez la console Amazon Macie ou l'API Amazon Macie, comme indiqué dans. Spécification de plusieurs valeurs pour un champ

Booléen

Spécifie l'une des deux valeurs mutuellement exclusives pour un champ.

Si vous utilisez la console Amazon Macie pour spécifier ce type de valeur, la console fournit une liste de valeurs parmi lesquelles choisir. Si vous utilisez l'API Amazon Macie, spécifiez `true` ou `false` pour la valeur.

Date/heure (et plages horaires)

Spécifie une date et une heure absolues pour un champ. Si vous spécifiez ce type de valeur, vous devez spécifier à la fois une date et une heure.

Sur la console Amazon Macie, les valeurs de date et d'heure sont indiquées dans votre fuseau horaire local et utilisent une notation de 24 heures. Dans tous les autres contextes, ces valeurs sont en temps universel coordonné (UTC) et au format ISO 8601 étendu, par exemple `2020-09-01T14:31:13Z` pour 14h31:13 UTC le 1er septembre 2020.

Si un champ contient une valeur de date/heure, vous pouvez l'utiliser pour définir une plage de temps fixe ou relative. Par exemple, vous pouvez inclure uniquement les résultats créés entre deux dates et heures spécifiques, ou uniquement les résultats créés avant ou après une date et une heure spécifiques. La façon dont vous définissez une plage horaire varie selon que vous utilisez la console Amazon Macie ou l'API Amazon Macie :

- Sur la console, utilisez un sélecteur de date ou saisissez du texte directement dans les champs From et To.
- Avec l'API, définissez une plage de temps fixe en ajoutant une condition qui spécifie la première date et l'heure de la plage, et ajoutez une autre condition qui spécifie la dernière date et heure de la plage. Si vous le faites, Macie utilise la logique AND pour joindre les conditions. Pour définir une plage de temps relative, ajoutez une condition qui spécifie la première ou la dernière date et heure de la plage. Spécifiez les valeurs sous forme d'horodatage Unix en millisecondes, par exemple, `1604616572653` pour le 5 novembre 2020 à 22:49:32 UTC.

Sur la console, les plages horaires sont inclusives. Avec l'API, les plages de temps peuvent être inclusives ou exclusives, selon l'opérateur que vous choisissez.

Nombre (et plages numériques)

Spécifie un entier long pour un champ.

Si un champ contient une valeur numérique, vous pouvez l'utiliser pour définir une plage numérique fixe ou relative. Par exemple, vous ne pouvez inclure que les résultats qui signalent 50 à 90 occurrences de données sensibles dans un objet S3. La façon dont vous définissez une plage numérique varie selon que vous utilisez la console Amazon Macie ou l'API Amazon Macie :

- Sur la console, utilisez les champs From et To pour saisir les nombres les plus bas et les plus élevés de la plage, respectivement.
- À l'aide de l'API, définissez une plage numérique fixe en ajoutant une condition spécifiant le nombre le plus bas de la plage, et ajoutez une autre condition spécifiant le nombre le plus élevé de la plage. Si vous le faites, Macie utilise la logique AND pour joindre les conditions. Pour définir une plage numérique relative, ajoutez une condition spécifiant le nombre le plus bas ou le plus élevé de la plage.

Sur la console, les plages numériques sont incluses. Avec l'API, les plages numériques peuvent être inclusives ou exclusives, selon l'opérateur que vous choisissez.

Texte (chaîne)

Spécifie une valeur de texte (chaîne) unique pour un champ. La chaîne est en corrélation avec une valeur prédéfinie ou existante pour un champ, par exemple, High pour le champ Severity, le nom d'un compartiment S3 pour le champ du nom du compartiment S3 ou l'identifiant unique d'une tâche de découverte de données sensibles pour le champ Job ID.

Si vous spécifiez une seule chaîne de texte, notez ce qui suit :

- Les valeurs distinguent les majuscules et minuscules.
- Vous ne pouvez pas utiliser de valeurs partielles ou de caractères génériques dans les valeurs. Vous devez spécifier une valeur complète et valide pour le champ.

Par exemple, pour filtrer les résultats d'un compartiment S3 nommé My-S3-bucket, entrez **`my-S3-bucket`** la valeur du champ Nom du compartiment S3. Si vous entrez une autre valeur, telle que **`my-s3-bucket`** ou**`my-S3`**, Macie ne renverra pas les résultats pour le bucket.

Pour obtenir la liste des valeurs valides pour chaque champ, consultezChamps pour filtrer les résultats.

Spécification de plusieurs valeurs pour un champ

Avec certains champs et opérateurs, vous pouvez spécifier plusieurs valeurs pour un champ. Dans ce cas, Macie utilise la logique OR pour joindre les valeurs et évaluer les critères de filtrage. Cela signifie qu'une recherche correspond aux critères si elle contient l'une des valeurs du champ.

Par exemple, si vous ajoutez une condition pour inclure des résultats dont la valeur du champ Type de recherche est égale à : S3Object/Financial SensitiveData,:S3Object/Personal, SensitiveData Macie renvoie des résultats de données sensibles pour les objets S3 contenant uniquement des informations financières et les objets S3 contenant uniquement des informations personnelles. En d'autres termes, Macie exclut toutes les conclusions des politiques. Macie exclut également toutes les découvertes de données sensibles pour les objets contenant d'autres types de données sensibles ou plusieurs types de données sensibles.

L'exception concerne les conditions qui utilisent l'eqExactMatchopérateur. Pour cet opérateur, Macie utilise la logique AND pour joindre les valeurs et évaluer les critères de filtre. Cela signifie qu'une recherche correspond aux critères uniquement si elle contient toutes les valeurs du champ et uniquement ces valeurs pour le champ. Pour en savoir plus sur cet opérateur, consultezUtilisation d'opérateurs dans des conditions.

La manière dont vous spécifiez plusieurs valeurs pour un champ dépend de votre utilisation de l'API Amazon Macie ou de la console Amazon Macie. Avec l'API, vous utilisez un tableau répertoriant les valeurs.

Sur la console, vous choisissez généralement les valeurs dans une liste. Toutefois, pour certains champs, vous devez ajouter une condition distincte pour chaque valeur. Par exemple, pour inclure les résultats relatifs aux données détectées par Macie à l'aide de certains identifiants de données personnalisés, procédez comme suit :

1. Placez votre curseur dans la zone Critères de filtre, puis choisissez le champ Nom de l'identifiant de données personnalisé. Entrez le nom d'un identifiant de données personnalisé, puis choisissez Appliquer.
2. Répétez l'étape précédente pour chaque identifiant de données personnalisé supplémentaire que vous souhaitez spécifier pour le filtre.

Pour obtenir la liste des champs pour lesquels vous devez effectuer cette opération, consultezChamps pour filtrer les résultats.

Utilisation d'opérateurs dans des conditions

Vous pouvez utiliser les types d'opérateurs suivants dans des conditions individuelles.

Égal à (eq)

Correspond à (=) n'importe quelle valeur spécifiée pour le champ. Vous pouvez utiliser l'opérateur égal avec les types de valeurs suivants : tableau de texte (chaînes), booléen, date/heure, nombre et texte (chaîne).

Pour de nombreux champs, vous pouvez utiliser cet opérateur et spécifier jusqu'à 50 valeurs pour le champ. Dans ce cas, Macie utilise la logique OR pour joindre les valeurs. Cela signifie qu'une recherche correspond aux critères si elle contient l'une des valeurs spécifiées pour le champ.

Par exemple :

- Pour inclure les résultats signalant la présence d'informations financières, d'informations personnelles ou à la fois d'informations financières et personnelles, ajoutez une condition utilisant le champ Catégorie de données sensibles et cet opérateur, et spécifiez Informations financières et Informations personnelles comme valeurs du champ.
- Pour inclure les résultats signalant la présence de numéros de carte de crédit, d'adresses postales ou à la fois de numéros de carte de crédit et d'adresses postales, ajoutez une condition pour le champ Type de détection de données sensibles, utilisez cet opérateur CREDIT_CARD_NUMBERet spécifiez et ADDRESScomme valeurs pour le champ.

Si vous utilisez l'API Amazon Macie pour définir une condition qui utilise cet opérateur avec une valeur de date/heure, spécifiez la valeur sous forme d'horodatage Unix en millisecondes, par exemple pour 22:49:32 UTC le 5 novembre 2020. `1604616572653`

Correspond à une correspondance exacte (eqExactMatch)

Correspond exclusivement à toutes les valeurs spécifiées pour le champ. Vous pouvez utiliser l'opérateur de correspondance exacte égale à un ensemble de champs sélectionnés.

Si vous utilisez cet opérateur et que vous spécifiez plusieurs valeurs pour un champ, Macie utilise la logique AND pour joindre les valeurs. Cela signifie qu'un résultat correspond aux critères uniquement s'il contient toutes les valeurs spécifiées pour le champ et uniquement ces valeurs pour le champ. Vous pouvez spécifier jusqu'à 50 valeurs pour le champ.

Par exemple :

- Pour inclure les résultats signalant des occurrences de numéros de carte de crédit et aucun autre type de données sensibles, ajoutez une condition pour le champ Type de détection de données sensibles, utilisez cet opérateur et spécifiez CREDIT_CARD_NUMBERcomme seule valeur pour le champ.

- Pour inclure les résultats signalant l'occurrence de numéros de carte de crédit et d'adresses postales (et aucun autre type de données sensibles), ajoutez une condition pour le champ Type de détection de données sensibles, utilisez cet opérateur CREDIT_CARD_NUMBERet spécifiez et ADDRESScomme valeurs pour le champ.

Comme Macie utilise la logique AND pour joindre les valeurs d'un champ, vous ne pouvez pas utiliser cet opérateur en combinaison avec d'autres opérateurs pour le même champ. En d'autres termes, si vous utilisez l'opérateur de correspondance exacte égale avec un champ dans une condition, vous devez l'utiliser dans toutes les autres conditions qui utilisent le même champ.

Comme les autres opérateurs, vous pouvez utiliser l'opérateur de correspondance exacte égale dans plusieurs conditions d'un filtre. Dans ce cas, Macie utilise la logique AND pour joindre les conditions et évaluer le filtre. Cela signifie qu'un résultat correspond aux critères du filtre uniquement s'il possède toutes les valeurs spécifiées par toutes les conditions du filtre.

Par exemple, pour inclure les résultats créés après un certain temps, signaler les occurrences de numéros de carte de crédit et ne signaler aucun autre type de données sensibles, procédez comme suit :

1. Ajoutez une condition qui utilise le champ Created at, utilise l'opérateur supérieur à et spécifie la date et l'heure de début du filtre.
2. Ajoutez une autre condition qui utilise le champ Type de détection de données sensibles, utilise l'opérateur de correspondance exacte égal et spécifie CREDIT_CARD_NUMBERcomme seule valeur pour le champ.

Vous pouvez utiliser l'opérateur de correspondance exacte égale avec les champs suivants :

- ID d'identifiant de données personnalisé (`customDataIdentifiers.detections.arn`)
- Nom de l'identifiant de données personnalisé (`customDataIdentifiers.detections.name`)
- clé d'identification du compartiment S3 (`resourcesAffected.s3Bucket.tags.key`)
- Valeur de la balise du compartiment S3 (`resourcesAffected.s3Bucket.tags.value`)
- clé de balise d'objet S3 (`resourcesAffected.s3Object.tags.key`)
- Valeur de la balise d'objet S3 (`resourcesAffected.s3Object.tags.value`)
- Type de détection de données sensibles (`sensitiveData.detections.type`)
- Catégorie de données sensibles (`sensitiveData.category`)

Dans la liste précédente, le nom entre parenthèses utilise la notation par points pour indiquer le nom du champ dans les représentations JSON des résultats et dans l'API Amazon Macie.

Supérieur à (gt)

Est supérieur à (**>**) la valeur spécifiée pour le champ. Vous pouvez utiliser l'opérateur supérieur à avec des valeurs numériques et date/heure.

Par exemple, pour inclure uniquement les résultats signalant plus de 90 occurrences de données sensibles dans un objet S3, ajoutez une condition qui utilise le champ Nombre total de données sensibles et cet opérateur, et spécifiez 90 comme valeur pour le champ. Pour ce faire, sur la console Amazon Macie, entrez **91** dans le champ De, ne saisissez aucune valeur dans le champ À, puis choisissez Appliquer. Les comparaisons numériques et temporelles sont incluses dans la console.

Si vous utilisez l'API Amazon Macie pour définir une plage horaire utilisant cet opérateur, vous devez spécifier les valeurs de date/heure sous forme d'horodatage Unix en millisecondes, par exemple pour 22:49:32 UTC le 5 novembre 2020. `1604616572653`

Supérieur ou égal à (gte)

Est supérieur ou égal à (**>=**) la valeur spécifiée pour le champ. Vous pouvez utiliser l'opérateur supérieur ou égal à pour les valeurs numériques et de date/heure.

Par exemple, pour inclure uniquement les résultats signalant au moins 90 occurrences de données sensibles dans un objet S3, ajoutez une condition qui utilise le champ Nombre total de données sensibles et cet opérateur, et spécifiez 90 comme valeur pour le champ. Pour ce faire, sur la console Amazon Macie, entrez **90** dans le champ De, ne saisissez aucune valeur dans le champ À, puis choisissez Appliquer.

Si vous utilisez l'API Amazon Macie pour définir une plage horaire utilisant cet opérateur, vous devez spécifier les valeurs de date/heure sous forme d'horodatage Unix en millisecondes, par exemple pour 22:49:32 UTC le 5 novembre 2020. `1604616572653`

Inférieur à (lt)

Est inférieur à (**<**) la valeur spécifiée pour le champ. Vous pouvez utiliser l'opérateur inférieur à avec des valeurs numériques et date/heure.

Par exemple, pour inclure uniquement les résultats signalant moins de 90 occurrences de données sensibles dans un objet S3, ajoutez une condition qui utilise le champ Nombre total de données sensibles et cet opérateur, et spécifiez 90 comme valeur pour le champ. Pour ce faire, sur la console Amazon Macie, entrez **89** dans le champ À, ne saisissez aucune valeur dans le champ De, puis choisissez Appliquer. Les comparaisons numériques et temporelles sont incluses dans la console.

Si vous utilisez l'API Amazon Macie pour définir une plage horaire utilisant cet opérateur, vous devez spécifier les valeurs de date/heure sous forme d'horodatage Unix en millisecondes, par exemple pour 22:49:32 UTC le 5 novembre 2020. `1604616572653`

Inférieur ou égal à (lte)

Est inférieur ou égal à (**<=**) la valeur spécifiée pour le champ. Vous pouvez utiliser l'opérateur inférieur ou égal à pour les valeurs numériques et de date/heure.

Par exemple, pour inclure uniquement les résultats signalant 90 occurrences ou moins de données sensibles dans un objet S3, ajoutez une condition qui utilise le champ Nombre total de données sensibles et cet opérateur, et spécifiez 90 comme valeur pour le champ. Pour ce faire, sur la console Amazon Macie, entrez **`90`** dans le champ À, ne saisissez aucune valeur dans le champ De, puis choisissez Appliquer.

Si vous utilisez l'API Amazon Macie pour définir une plage horaire utilisant cet opérateur, vous devez spécifier les valeurs de date/heure sous forme d'horodatage Unix en millisecondes, par exemple pour 22:49:32 UTC le 5 novembre 2020. `1604616572653`

Non égal à (neq)

Ne correspond à aucune valeur spécifiée pour le champ. Vous pouvez utiliser l'opérateur différent avec les types de valeurs suivants : tableau de texte (chaînes), booléen, date/heure, nombre et texte (chaîne).

Pour de nombreux champs, vous pouvez utiliser cet opérateur et spécifier jusqu'à 50 valeurs pour le champ. Dans ce cas, Macie utilise la logique OR pour joindre les valeurs. Cela signifie qu'un résultat correspond aux critères s'il ne contient aucune des valeurs spécifiées pour le champ.

Par exemple :

- Pour exclure les résultats signalant la présence d'informations financières, d'informations personnelles ou à la fois d'informations financières et personnelles, ajoutez une condition utilisant le champ Catégorie de données sensibles et cet opérateur, et spécifiez Informations financières et Informations personnelles comme valeurs du champ.
- Pour exclure les résultats signalant des occurrences de numéros de carte de crédit, ajoutez une condition pour le champ Type de détection de données sensibles, utilisez cet opérateur et spécifiez CREDIT_CARD_NUMBERla valeur du champ.
- Pour exclure les résultats signalant la présence de numéros de carte de crédit, d'adresses postales ou à la fois de numéros de carte de crédit et d'adresses postales, ajoutez une

condition pour le champ Type de détection de données sensibles, utilisez cet opérateur CREDIT_CARD_NUMBERet spécifiez et ADDRESScomme valeurs pour le champ.

Si vous utilisez l'API Amazon Macie pour définir une condition qui utilise cet opérateur avec une valeur de date/heure, spécifiez la valeur sous forme d'horodatage Unix en millisecondes, par exemple pour 22:49:32 UTC le 5 novembre 2020. `1604616572653`

Création et application de filtres aux résultats

Pour identifier et cibler les résultats présentant des caractéristiques spécifiques, vous pouvez filtrer les résultats sur la console Amazon Macie et dans les requêtes que vous soumettez par programmation à l'aide de l'API Amazon Macie. Lorsque vous créez un filtre, vous utilisez des attributs spécifiques des résultats pour définir des critères permettant d'inclure ou d'exclure les résultats d'une vue ou des résultats de requête. Un attribut de recherche est un champ qui stocke des données spécifiques pour un résultat, telles que la gravité, le type ou le nom du compartiment S3 auquel le résultat s'applique.

Dans Macie, un filtre comprend une ou plusieurs conditions. Chaque condition, également appelée critère, comprend trois parties :

- Champ basé sur un attribut, tel que le niveau de gravité ou le type de recherche.
- Un opérateur, tel que égal ou non égal.
- Une ou plusieurs valeurs. Le type et le nombre de valeurs dépendent du champ et de l'opérateur que vous choisissez.

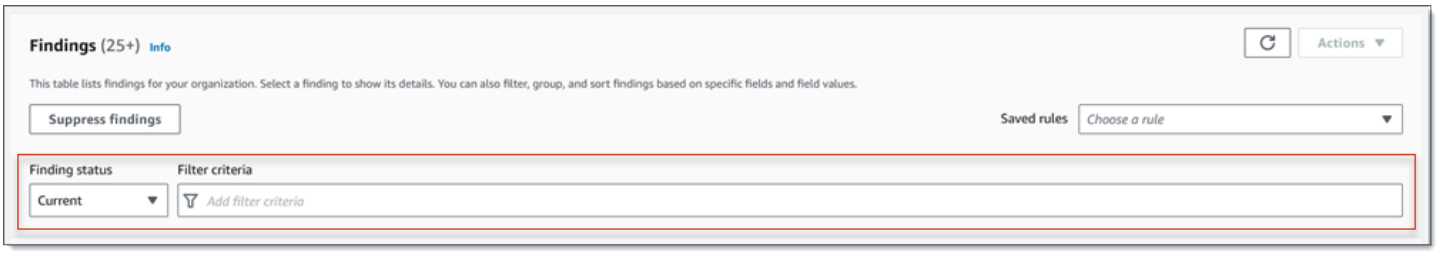
La façon dont vous définissez et appliquez les conditions de filtrage dépend de votre utilisation de la console Amazon Macie ou de l'API Amazon Macie.

Rubriques

Filtrer les résultats sur la console Amazon Macie

Si vous utilisez la console Amazon Macie pour filtrer les résultats, Macie propose des options pour vous aider à choisir des champs, des opérateurs et des valeurs pour des conditions individuelles.

Vous pouvez accéder à ces options en utilisant les paramètres de filtre sur les pages de résultats, comme illustré dans l'image suivante.



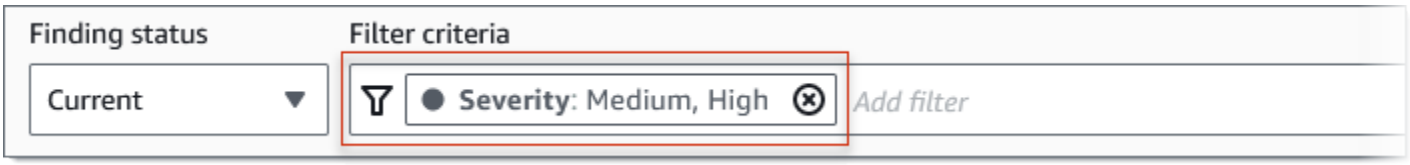
À l'aide du menu État de la recherche, vous pouvez indiquer si vous souhaitez inclure les résultats supprimés (archivés automatiquement) par une règle de suppression. À l'aide de la zone Critères de filtre, vous pouvez saisir les conditions du filtre.

Lorsque vous placez votre curseur dans la zone Critères de filtre, Macie affiche une liste de champs que vous pouvez utiliser dans des conditions de filtrage. Les champs sont organisés par catégorie logique. Par exemple, la catégorie Champs communs inclut des champs qui s'appliquent à tout type de recherche, et la catégorie Champs de classification inclut des champs qui s'appliquent uniquement aux résultats de données sensibles. Les champs sont triés par ordre alphabétique au sein de chaque catégorie.

Pour ajouter une condition, commencez par choisir un champ dans la liste. Pour trouver un champ, parcourez la liste complète ou entrez une partie du nom du champ pour affiner la liste des champs.

Selon le champ que vous choisissez, Macie affiche différentes options. Les options reflètent le type et la nature du champ que vous choisissez. Par exemple, si vous choisissez le champ Sévérité, Macie affiche une liste de valeurs parmi lesquelles choisir : faible, moyen et élevé. Si vous choisissez le champ Nom du compartiment S3, Macie affiche une zone de texte dans laquelle vous pouvez saisir un nom de compartiment. Quel que soit le champ que vous choisissez, Macie vous guide à travers les étapes pour ajouter une condition incluant les paramètres requis pour le champ.

Après avoir ajouté une condition, Macie applique les critères de la condition et ajoute la condition à un jeton de filtre dans la zone Critères de filtre, comme illustré dans l'image suivante.



Dans cet exemple, la condition est configurée pour inclure tous les résultats de gravité moyenne et élevée, et pour exclure tous les résultats de gravité faible. Elle renvoie des résultats pour lesquels la valeur du champ Sévérité est égale à moyenne ou élevée.

> **Tip**
>
> Pour de nombreux champs, vous pouvez modifier l'opérateur d'une condition de égal à non égal en choisissant l'icône égal (●) dans le jeton de filtre correspondant à la condition. Dans ce cas, Macie remplace l'opérateur par not equal et affiche l'icône « not equal » (⊘) dans le jeton. Pour revenir à l'opérateur égal, cliquez sur l'icône « Pas égal ».

Au fur et à mesure que vous ajoutez des conditions, Macie applique leurs critères et les ajoute aux jetons dans la zone Critères de filtrage. Vous pouvez consulter la case à tout moment pour déterminer les critères que vous avez appliqués. Pour supprimer une condition, cliquez sur l'icône de suppression de la condition (⊗) dans le jeton correspondant à la condition.

Pour filtrer les résultats à l'aide de la console

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Conclusions.
3. (Facultatif) Pour d'abord passer en revue les résultats d'un groupe logique prédéfini et les examiner, choisissez Par compartiment, Par type ou Par tâche dans le volet de navigation (sous Résultats). Choisissez ensuite un élément dans le tableau. Dans le panneau de détails, choisissez le lien vers lequel le champ doit être pivoté.
4. (Facultatif) Pour afficher les résultats supprimés par une règle de suppression, modifiez le paramètre d'état du filtre. Choisissez Archivé pour afficher uniquement les résultats supprimés, ou choisissez Tout pour afficher à la fois les résultats supprimés et non supprimés. Pour masquer les résultats supprimés, choisissez Current.
5. Pour ajouter une condition de filtre :
   a. Placez votre curseur dans la zone Critères de filtre, puis choisissez le champ à utiliser pour la condition. Pour plus d'informations sur les champs que vous pouvez utiliser, consultezChamps pour filtrer les résultats.

b. Entrez le type de valeur approprié pour le champ. Pour des informations détaillées sur les différents types de valeurs, consultezSpécification de valeurs pour les champs.

Tableau de texte (chaînes)

Pour ce type de valeur, Macie fournit souvent une liste de valeurs parmi lesquelles choisir. Dans ce cas, sélectionnez chaque valeur que vous souhaitez utiliser dans la condition.

Si Macie ne fournit pas de liste de valeurs, entrez une valeur complète et valide pour le champ. Pour spécifier des valeurs supplémentaires pour le champ, choisissez Appliquer, puis ajoutez une autre condition pour chaque valeur supplémentaire.

Notez que les valeurs distinguent les majuscules et minuscules. En outre, vous ne pouvez pas utiliser de valeurs partielles ou de caractères génériques dans les valeurs. Par exemple, pour filtrer les résultats d'un compartiment S3 nommé My-S3-bucket, entrez **`my-S3-bucket`** la valeur du champ Nom du compartiment S3. Si vous entrez une autre valeur, telle que **`my-s3-bucket`** ou**`my-S3`**, Macie ne renverra pas les résultats pour le bucket.

Booléen

Pour ce type de valeur, Macie fournit une liste de valeurs parmi lesquelles choisir. Sélectionnez la valeur que vous souhaitez utiliser dans la condition.

Date/heure (plages horaires)

Pour ce type de valeur, utilisez les champs From et To pour définir une plage de temps inclusive :

- Pour définir une plage horaire fixe, utilisez les champs From et To pour spécifier la première date et l'heure ainsi que les dernières date et heure de la plage, respectivement.
- Pour définir une plage de temps relative qui commence à une certaine date et heure et se termine à l'heure actuelle, entrez la date et l'heure de début dans les zones De et supprimez tout texte dans les zones À.
- Pour définir une plage de temps relative se terminant à une certaine date et heure, entrez la date et l'heure de fin dans les zones À et supprimez le texte dans les zones De.

Notez que les valeurs temporelles utilisent une notation de 24 heures. Si vous utilisez le sélecteur de dates pour choisir des dates, vous pouvez affiner les valeurs en saisissant du texte directement dans les zones De et À.

Nombre (plages numériques)

Pour ce type de valeur, utilisez les champs From et To pour saisir un ou plusieurs entiers qui définissent une plage numérique inclusive, fixe ou relative.

Valeurs de texte (chaîne)

Pour ce type de valeur, entrez une valeur complète et valide pour le champ.

Notez que les valeurs distinguent les majuscules et minuscules. En outre, vous ne pouvez pas utiliser de valeurs partielles ou de caractères génériques dans les valeurs. Par exemple, pour filtrer les résultats d'un compartiment S3 nommé My-S3-bucket, entrez **`my-S3-bucket`** la valeur du champ Nom du compartiment S3. Si vous entrez une autre valeur, telle que **`my-s3-bucket`** ou**`my-S3`**, Macie ne renverra pas les résultats pour le bucket.

c. Lorsque vous avez fini d'ajouter des valeurs pour le champ, choisissez Appliquer. Macie applique les critères de filtre et ajoute la condition à un jeton de filtre dans la zone Critères de filtre.

6. Répétez l'étape 5 pour chaque condition supplémentaire que vous souhaitez ajouter.
7. Pour supprimer une condition, cliquez sur l'icône de suppression de la condition (⊗) dans le jeton de filtre correspondant à la condition.
8. Pour modifier une condition, supprimez-la en cliquant sur l'icône de suppression de la condition (⊗) dans le jeton de filtre correspondant à la condition. Répétez ensuite l'étape 5 pour ajouter une condition avec les bons paramètres.

Si vous souhaitez réutiliser cet ensemble de conditions par la suite, vous pouvez l'enregistrer en tant que règle de filtre. Pour ce faire, choisissez Enregistrer la règle dans la zone Critères de filtrage. Entrez ensuite un nom et, éventuellement, une description pour la règle. Lorsque vous avez terminé, choisissez Enregistrer.

Filtrer les résultats par programmation à l'aide de l'API Amazon Macie

Pour filtrer les résultats par programmation, spécifiez des critères de filtrage dans les requêtes que vous soumettez à l'aide de l'API Amazon Macie ListFindingsGetFindingStatisticsou à l'aide de celle-ci. L'ListFindingsopération renvoie un tableau d'identifiants de recherche, un identifiant pour chaque résultat correspondant aux critères du filtre. L'GetFindingStatisticsopération renvoie des données statistiques agrégées concernant tous les résultats correspondant aux critères du filtre, regroupés selon un champ que vous spécifiez dans votre demande.

Notez que les GetFindingStatistics opérations ListFindings et sont différentes des opérations que vous utilisez pour supprimer les résultats. Contrairement aux opérations de suppression, qui spécifient également des critères de filtre, les GetFindingStatistics opérations ListFindings et interrogent uniquement les données de résultats. Ils n'exécutent aucune action sur les résultats correspondant aux critères du filtre. Pour supprimer les résultats, utilisez le CreateFindingsFilterfonctionnement de l'API Amazon Macie.

Pour spécifier des critères de filtre dans une requête, incluez une carte des conditions de filtre dans votre demande. Pour chaque condition, spécifiez un champ, un opérateur et une ou plusieurs valeurs pour le champ. Le type et le nombre de valeurs dépendent du champ et de l'opérateur que vous choisissez. Pour plus d'informations sur les champs, les opérateurs et les types de valeurs que vous pouvez utiliser dans une condition Champs pour filtrer les résultatsUtilisation d'opérateurs dans des conditions, reportez-vous aux sections etSpécification de valeurs pour les champs.

Les exemples suivants vous montrent comment spécifier des critères de filtre dans les requêtes que vous soumettez à l'aide du AWS Command Line Interface(AWS CLI). Vous pouvez également le faire en utilisant une version actuelle d'un autre outil de ligne de AWS commande ou d'un AWS SDK, ou en envoyant des requêtes HTTPS directement à Macie. Pour plus d'informations sur AWS les outils et les SDK, consultez la section Outils sur AWS lesquels vous pouvez vous appuyer.

Exemples

- Exemple 1 : Filtrer les résultats en fonction de leur gravité
- Exemple 2 : Filtrer les résultats en fonction de la catégorie de données sensibles
- Exemple 3 : Filtrer les résultats en fonction d'une plage de temps fixe
- Exemple 4 : Filtrer les résultats en fonction de l'état de suppression
- Exemple 5 : Filtrer les résultats en fonction de plusieurs champs et types de valeurs

Les exemples utilisent la commande list-findings. Si un exemple s'exécute correctement, Macie renvoie un `findingIds` tableau. Le tableau répertorie l'identifiant unique pour chaque résultat correspondant aux critères du filtre, comme illustré dans l'exemple suivant.

```
{
    "findingIds": [
        "1f1c2d74db5d8caa76859ec52example",
        "6cfa9ac820dd6d55cad30d851example",
        "702a6fd8750e567d1a3a63138example",
        "826e94e2a820312f9f964cf60example",
        "274511c3fdcd87010a19a3a42example"
    ]
}
```

Si aucun résultat ne correspond aux critères du filtre, Macie renvoie un `findingIds` tableau vide.

```
{
    "findingIds": []
}
```

Exemple 1 : Filtrer les résultats en fonction de leur gravité

Cet exemple utilise la commande list-findings pour récupérer les identifiants de recherche pour tous vos résultats de gravité élevée et moyenne du moment. Région AWS

Pour Linux, macOS ou Unix :

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"severity.description":
{"eq":["High","Medium"]}}}'
```

Pour Microsoft Windows :

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":
{\"severity.description\":{\"eq\":[\"High\",\"Medium\"]}}}
```

Où :

- *severity.description* indique le nom JSON du champ Severity.
- *eq* spécifie l'opérateur égal.

- *High* et *Medium* sont un tableau de valeurs énumérées pour le champ Severity.

Exemple 2 : Filtrer les résultats en fonction de la catégorie de données sensibles

Cet exemple utilise la commande list-findings pour récupérer les identifiants de recherche pour toutes vos découvertes de données sensibles qui se trouvent dans la région actuelle et pour signaler les occurrences d'informations financières (et aucune autre catégorie de données sensibles) dans des objets S3.

Pour Linux, macOS ou Unix, utilisez la barre oblique inverse (\) pour améliorer la lisibilité :

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["FINANCIAL_INFORMATION"]}}}'
```

Pour Microsoft Windows, utilisez le caractère de continuation de ligne caret (^) pour améliorer la lisibilité :

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.category\":{\"eqExactMatch\":
[\"FINANCIAL_INFORMATION\"]}}}
```

Où :

- *ClassificationDetails.Result.SensitiveData.Category spécifie le nom JSON du champ de catégorie* de données sensibles.
- *eqExactMatch*spécifie l'opérateur de correspondance exacte égal à égal.
- *FINANCIAL_INFORMATION* est une valeur énumérée pour le champ de catégorie de données sensibles.

Exemple 3 : Filtrer les résultats en fonction d'une plage de temps fixe

Cet exemple utilise la commande list-findings pour récupérer les identifiants de recherche pour tous vos résultats qui se trouvent dans la région actuelle et ont été créés entre 7 h 00 UTC le 5 octobre 2020 et 7 h 00 UTC le 5 novembre 2020 (inclus).

Pour Linux, macOS ou Unix :

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"createdAt":
{"gte":1601881200000,"lte":1604559600000}}}'
```

Pour Microsoft Windows :

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"createdAt\":
{\"gte\":1601881200000,\"lte\":1604559600000}}}
```

Où :

- *CreatedAt* spécifie le nom JSON du champ Created at.
- *gte* spécifie l'opérateur supérieur ou égal à.
- *1601881200000* est la première date et heure (sous forme d'horodatage Unix en millisecondes) de la plage horaire.
- *lte* spécifie l'opérateur inférieur ou égal à.
- *1604559600000 correspond* à la dernière date et heure (sous forme d'horodatage Unix en millisecondes) de la plage horaire.

Exemple 4 : Filtrer les résultats en fonction de l'état de suppression

Cet exemple utilise la commande list-findings pour récupérer les identifiants de recherche pour tous vos résultats qui se trouvent dans la région actuelle et qui ont été supprimés (archivés automatiquement) par une règle de suppression.

Pour Linux, macOS ou Unix :

```
$ aws macie2 list-findings --finding-criteria '{"criterion":{"archived":{"eq":
["true"]}}}'
```

Pour Microsoft Windows :

```
C:\> aws macie2 list-findings --finding-criteria={\"criterion\":{\"archived\":{\"eq\":
[\"true\"]}}}
```

Où :

- *archivé* indique le nom JSON du champ Archivé.
- *eq* spécifie l'opérateur égal.

- *true* est une valeur booléenne pour le champ Archivé.

Exemple 5 : Filtrer les résultats en fonction de plusieurs champs et types de valeurs

Cet exemple utilise la commande list-findings pour récupérer les identifiants de recherche pour toutes vos découvertes de données sensibles qui se trouvent dans la région actuelle et répondent aux critères suivants : ont été créées entre 07h00 UTC le 5 octobre 2020 et 07h00 UTC le 5 novembre 2020 (exclusivement) ; signalent les occurrences de données financières et aucune autre catégorie de données sensibles dans les objets S3 ; et n'ont pas été supprimées (archivées automatiquement) par une règle de suppression.

Pour Linux, macOS ou Unix, utilisez la barre oblique inverse (\) pour améliorer la lisibilité :

```
$ aws macie2 list-findings \
--finding-criteria '{"criterion":{"createdAt":
{"gt":1601881200000,"lt":1604559600000},"classificationDetails.result.sensitiveData.category":
{"eqExactMatch":["FINANCIAL_INFORMATION"]},"archived":{"eq":["false"]}}}'
```

Pour Microsoft Windows, utilisez le caractère de continuation de ligne caret (^) pour améliorer la lisibilité :

```
C:\> aws macie2 list-findings ^
--finding-criteria={\"criterion\":{\"createdAt\":{\"gt\":1601881200000,
\"lt\":1604559600000},\"classificationDetails.result.sensitiveData.category\":
{\"eqExactMatch\":[\"FINANCIAL_INFORMATION\"]},\"archived\":{\"eq\":[\"false\"]}}}
```

Où :

- *CreatedAt* spécifie le nom JSON du champ Created at et :
  - *gt* spécifie l'opérateur supérieur ou égal à.
  - *1601881200000* est la première date et heure (sous forme d'horodatage Unix en millisecondes) de la plage horaire.
  - *lt* spécifie l'opérateur inférieur ou égal à.
  - *1604559600000 correspond* à la dernière date et heure (sous forme d'horodatage Unix en millisecondes) de la plage horaire.
- *ClassificationDetails.Result.SensitiveData.Category spécifie le nom JSON du champ de catégorie* de données sensibles et :
  - *eqExactMatch*spécifie l'opérateur de correspondance exacte égal à égal.

    - `FINANCIAL_INFORMATION` est une valeur énumérée pour le champ.
- `archivé` indique le nom JSON du champ Archivé, et :
    - `eq` spécifie l'opérateur égal.
    - `false` est une valeur booléenne pour le champ.

Création et gestion de règles de filtrage pour les résultats

Une règle de filtrage est un ensemble de critères de filtre que vous créez et enregistrez pour réutiliser lorsque vous consultez les résultats sur la console Amazon Macie. Les règles de filtrage peuvent vous aider à effectuer une analyse cohérente des résultats présentant des caractéristiques spécifiques. Par exemple, vous pouvez créer une règle de filtre pour analyser toutes les conclusions de politique de gravité élevée pour les compartiments S3 contenant des objets non chiffrés, et une autre règle de filtre pour analyser toutes les conclusions de données sensibles de gravité élevée signalant des types spécifiques de données sensibles.

Notez que les règles de filtrage sont différentes des règles de suppression. Une règle de suppression est un ensemble de critères de filtre que vous créez et enregistrez pour archiver automatiquement les résultats correspondant aux critères de la règle. Bien que les deux types de règles stockent et appliquent des critères de filtre, une règle de filtre n'effectue aucune action sur les résultats correspondant aux critères de la règle. Au lieu de cela, une règle de filtrage détermine uniquement les résultats qui apparaissent sur la console une fois que vous l'avez appliquée. Pour plus d'informations sur les règles de suppression, consultezSuppression de résultats.

Pour créer et gérer des règles de filtrage, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie. Les rubriques suivantes expliquent comment procéder. Pour l'API, les rubriques incluent des exemples expliquant comment effectuer ces tâches à l'aide de AWS Command Line Interface(AWS CLI). Vous pouvez également effectuer ces tâches en utilisant la version actuelle d'un autre outil de ligne de AWS commande ou d'un AWS SDK, ou en envoyant des requêtes HTTPS directement à Macie. Pour plus d'informations sur AWS les outils et les SDK, voir Outils sur AWS lesquels s'appuyer.

Rubriques

- Création de règles de filtrage
- Appliquer des règles de filtrage
- Modification des règles de filtrage
- Supprimer des règles de filtrage

Création de règles de filtrage

Lorsque vous créez une règle de filtre, vous spécifiez des critères de filtre, un nom et, éventuellement, une description de la règle. Vous pouvez créer une règle de filtrage à l'aide de la console Amazon Macie ou de l'API Amazon Macie.

Console

Suivez ces étapes pour créer une règle de filtrage à l'aide de la console Amazon Macie.

Pour créer une règle de filtrage

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Conclusions.

> **Tip**
>
> Pour utiliser une règle de filtre existante comme point de départ, choisissez-la dans la liste Règles enregistrées.
> Vous pouvez également rationaliser la création d'une règle en faisant d'abord pivoter et en analysant les résultats par un groupe logique prédéfini. Dans ce cas, Macie crée et applique automatiquement les conditions de filtre appropriées, ce qui peut constituer un point de départ utile pour créer une règle. Pour ce faire, choisissez Par compartiment, Par type ou Par tâche dans le volet de navigation (sous Résultats), puis choisissez un élément dans le tableau. Dans le panneau de détails, choisissez le lien vers lequel le champ doit être pivoté.

3. Dans la zone Critères de filtre, ajoutez des conditions qui définissent les critères de filtre pour la règle.

Pour savoir comment ajouter des conditions de filtre, voirCréation et application de filtres aux résultats.

4. Lorsque vous avez fini de définir les critères de filtre pour la règle, choisissez Enregistrer la règle dans la zone Critères de filtre.

5. Sous Règle de filtrage, entrez un nom et, éventuellement, une description de la règle.
6. Choisissez Save (Enregistrer).

API

Pour créer une règle de filtrage par programmation, utilisez le CreateFindingsFilterfonctionnement de l'API Amazon Macie et spécifiez les valeurs appropriées pour les paramètres requis :

- Pour le `action` paramètre, spécifiez `NOOP` pour vous assurer que Macie ne supprime pas (n'archive pas automatiquement) les résultats correspondant aux critères de la règle.
- Pour le `criterion` paramètre, spécifiez une carte des conditions qui définissent les critères de filtre pour la règle.

  Dans la carte, chaque condition doit spécifier un champ, un opérateur et une ou plusieurs valeurs pour le champ. Le type et le nombre de valeurs dépendent du champ et de l'opérateur que vous choisissez. Pour plus d'informations sur les champs, les opérateurs et les types de valeurs que vous pouvez utiliser dans une condition Champs pour filtrer les résultatsUtilisation d'opérateurs dans des conditions, reportez-vous aux sections etSpécification de valeurs pour les champs.

Pour créer une règle de filtre à l'aide deAWS CLI, exécutez la create-findings-filtercommande et spécifiez les valeurs appropriées pour les paramètres requis. Les exemples suivants créent une règle de filtre qui renvoie toutes les données sensibles trouvées dans la version actuelle Région AWS et signalent les occurrences d'informations personnelles (et aucune autre catégorie de données sensibles) dans les objets S3.

Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne inversée (\) pour améliorer la lisibilité.

```
$ aws macie2 create-findings-filter \
```

```
--action NOOP \
--name my_filter_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.category":{"eqExactMatch":
["PERSONAL_INFORMATION"]}}}'
```

Cet exemple est formaté pour Microsoft Windows et utilise le caractère de continuation de ligne caret (^) pour améliorer la lisibilité.

```
C:\> aws macie2 create-findings-filter ^
--action NOOP ^
--name my_filter_rule ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.category\":{\"eqExactMatch\":
[\"PERSONAL_INFORMATION\"]}}}
```

Où :

- *my_filter_rule* est le nom personnalisé de la règle.
- `criterion`est une carte des conditions de filtrage pour la règle :
  - *ClassificationDetails.Result.SensitiveData.Category est le nom JSON du champ de catégorie* de données sensibles.
  - *eqExactMatch*spécifie l'opérateur de correspondance exacte égal à égal.
  - *PERSONAL_INFORMATION* est une valeur énumérée pour le champ de catégorie de données sensibles.

Si la commande s'exécute correctement, vous recevez une sortie similaire à ce qui suit.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-
aa2f-4940-b347-d1451example",
    "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

Où se `arn` trouve le nom de ressource Amazon (ARN) de la règle de filtre créée et `id` l'identifiant unique de la règle.

Pour d'autres exemples de critères de filtre, voirFiltrer les résultats par programmation à l'aide de l'API Amazon Macie.

Appliquer des règles de filtrage

Lorsque vous appliquez une règle de filtrage, Amazon Macie utilise les critères de la règle pour déterminer les résultats à inclure ou à exclure de votre affichage des résultats sur la console. Macie affiche également les critères pour vous aider à déterminer les critères que vous avez appliqués.

Notez que les règles de filtrage sont conçues pour être utilisées avec la console Amazon Macie. Vous ne pouvez pas les utiliser directement dans les requêtes que vous soumettez par programmation à l'aide de l'API Amazon Macie. Toutefois, si vous utilisez l'API pour interroger les résultats, vous pouvez récupérer les critères de filtre d'une règle à l'aide de l'GetFindingsFilteropération. Vous pouvez ensuite ajouter les critères à votre requête. Pour plus d'informations sur la définition de critères de filtre dans une requête, consultezCréation et application de filtres aux résultats.

Procédez comme suit pour filtrer les résultats sur la console en appliquant une règle de filtrage.

Pour appliquer une règle de filtrage

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Conclusions.
3. Dans la liste Règles enregistrées, choisissez la règle de filtre que vous souhaitez appliquer. Macie applique les critères de la règle et affiche les critères dans la zone Critères de filtre.
4. (Facultatif) Pour affiner les critères, utilisez la zone Critères de filtre pour ajouter ou supprimer des conditions de filtre. Dans ce cas, vos modifications n'affecteront pas les paramètres de la règle. Macie n'enregistrera aucune de vos modifications, sauf si vous les enregistrez explicitement en tant que nouvelle règle.
5. Pour appliquer une autre règle de filtrage, répétez l'étape 3.

Après avoir appliqué une règle de filtre, vous pouvez rapidement supprimer tous ses critères de filtre de votre vue en choisissant le X dans la zone Critères de filtre.

Modification des règles de filtrage

Vous pouvez modifier les paramètres d'une règle de filtrage à tout moment à l'aide de la console Amazon Macie ou de l'API Amazon Macie. Vous pouvez également attribuer et gérer des balises pour la règle.

Un tag est un label que vous définissez et attribuez à certains types de AWS ressources. Chaque balise comprend une clé de balise obligatoire et une valeur de balise facultative. Les balises peuvent

vous aider à identifier, à classer et à gérer les ressources de différentes manières, par exemple en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Pour en savoir plus, consultez Marquage des ressources Amazon Macie.

Console

Suivez ces étapes pour modifier les paramètres d'une règle de filtre existante à l'aide de la console Amazon Macie.

Pour modifier une règle de filtrage

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Conclusions.
3. Dans la liste des règles enregistrées, cliquez sur l'icône de modification () à côté de la règle de filtre que vous souhaitez modifier.
4. Effectuez l'une des actions suivantes :
   - Pour modifier les critères de filtrage de la règle, utilisez la zone Critères de filtre pour entrer les conditions correspondant aux critères souhaités. Pour savoir comment procéder, veuillez consulter la section Création et application de filtres aux résultats.
   - Pour modifier le nom de la règle, entrez un nouveau nom dans le champ Nom sous Règle de filtrage.
   - Pour modifier la description de la règle, entrez une nouvelle description dans la zone Description sous Règle de filtrage.
   - Pour attribuer, vérifier ou modifier des balises pour la règle, choisissez Gérer les balises sous Règle de filtrage. Passez ensuite en revue et modifiez les balises si nécessaire. Une règle peut comporter jusqu'à 50 balises.
5. Une fois les modifications terminées, choisissez Save (Enregistrer).

API

Pour modifier une règle de filtre par programmation, utilisez le UpdateFindingsFilterfonctionnement de l'API Amazon Macie. Lorsque vous soumettez votre demande, utilisez les paramètres pris en charge pour spécifier une nouvelle valeur pour chaque paramètre que vous souhaitez modifier.

Pour le `id` paramètre, spécifiez l'identifiant unique de la règle à modifier. Vous pouvez obtenir cet identifiant en utilisant l'ListFindingsFilteropération pour récupérer une liste de règles de filtrage et de suppression pour votre compte. Si vous utilisez leAWS CLI, exécutez la list-findings-filterscommande pour récupérer cette liste.

Pour modifier une règle de filtre à l'aide deAWS CLI, exécutez la update-findings-filtercommande et utilisez les paramètres pris en charge pour spécifier une nouvelle valeur pour chaque paramètre que vous souhaitez modifier. Par exemple, la commande suivante modifie le nom d'une règle de filtre existante.

```
C:\> aws macie2 update-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example --
name personal_information_only
```

Où :

- *9b2b4508-aa2f-4940-b347-d1451example* est l'identifiant unique de la règle.
- *personal_information_only* est le nouveau nom de la règle.

Si la commande s'exécute correctement, vous recevez une sortie similaire à ce qui suit.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/9b2b4508-
aa2f-4940-b347-d1451example",
    "id": "9b2b4508-aa2f-4940-b347-d1451example"
}
```

Où se `arn` trouve le nom de ressource Amazon (ARN) de la règle modifiée et `id` l'identifiant unique de la règle.

De même, l'exemple suivant convertit une règle de suppression en règle de filtre en modifiant la valeur du `action` paramètre de `ARCHIVE` à`NOOP`.

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --
action NOOP
```

Où :

- *8a1c3508-aa2f-4940-b347-d1451example* est l'identifiant unique de la règle.

- Le *NOOP* est la nouvelle action que Macie doit exécuter sur les résultats qui répondent aux critères de la règle : n'effectuer aucune action (ne pas supprimer les résultats).

Si la commande s'exécute correctement, vous recevez un résultat similaire à ce qui suit :

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-
aa2f-4940-b347-d1451example",
    "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

Où se `arn` trouve le nom de ressource Amazon (ARN) de la règle modifiée et `id` l'identifiant unique de la règle.

Supprimer des règles de filtrage

Vous pouvez supprimer une règle de filtrage à tout moment à l'aide de la console Amazon Macie ou de l'API Amazon Macie.

Console

Suivez ces étapes pour supprimer une règle de filtrage à l'aide de la console Amazon Macie.

Pour supprimer une règle de filtrage

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Conclusions.
3. Dans la liste des règles enregistrées, cliquez sur l'icône de modification () à côté de la règle de filtre que vous souhaitez supprimer.
4. Sous Règle de filtrage, choisissez Supprimer.

API

Pour supprimer une règle de filtre par programmation, utilisez l'DeleteFindingsFilterAPI Amazon Macie. Pour le `id` paramètre, spécifiez l'identifiant unique de la règle de filtre à supprimer. Vous pouvez obtenir cet identifiant en utilisant l'ListFindingsFilteropération pour récupérer une liste de

règles de filtrage et de suppression pour votre compte. Si vous utilisez leAWS CLI, exécutez la list-findings-filterscommande pour récupérer cette liste.

Pour supprimer une règle de filtre à l'aide deAWS CLI, exécutez la delete-findings-filtercommande. Par exemple :

```
C:\> aws macie2 delete-findings-filter --id 9b2b4508-aa2f-4940-b347-d1451example
```

Où *9b2b4508-aa2f-4940-b347-d1451example* est l'identifiant unique de la règle de filtre à supprimer.

Si la commande s'exécute correctement, Macie renvoie une réponse HTTP 200 vide. Sinon, Macie renvoie une réponse HTTP 4 xx ou 500 indiquant pourquoi l'opération a échoué.

Champs pour filtrer les résultats

Pour vous aider à analyser les résultats de manière plus efficace, la console Amazon Macie et l'API Amazon Macie donnent accès à plusieurs ensembles de champs pour filtrer les résultats :

- Champs communs : ces champs stockent des données qui s'appliquent à tout type de recherche. Ils sont corrélés aux attributs communs des résultats tels que la gravité, le type de découverte et l'identifiant du résultat.
- Champs de ressources concernés : ces champs stockent des données relatives aux ressources auxquelles s'applique une recherche, telles que le nom, les balises et les paramètres de chiffrement d'un compartiment ou d'un objet S3 concerné.
- Champs de stratégie : ces champs stockent des données spécifiques aux conclusions des politiques, telles que l'action qui a produit une constatation et l'entité qui a effectué l'action.
- Champs de classification des données sensibles : ces champs stockent des données spécifiques aux résultats de données sensibles, telles que la catégorie et le type de données sensibles que Macie a trouvées dans un objet S3 concerné.

Un filtre peut utiliser une combinaison de champs provenant de n'importe lequel des ensembles précédents.

Les rubriques de cette section répertorient et décrivent les champs individuels que vous pouvez utiliser pour filtrer les résultats. Pour plus de détails sur ces champs, y compris les relations entre les champs, consultez les résultats du manuel Amazon Macie API Reference.

Rubriques

Champs communs

Le tableau suivant répertorie et décrit les champs que vous pouvez utiliser pour filtrer les résultats en fonction des attributs de recherche courants. Ces champs stockent des données qui s'appliquent à tout type de recherche.

Dans le tableau, la colonne Champ indique le nom du champ sur la console Amazon Macie. La colonne de champ JSON utilise la notation par points pour indiquer le nom du champ dans les représentations JSON des résultats et dans l'API Amazon Macie. La colonne Description fournit une brève description des données stockées dans le champ et indique les exigences relatives aux valeurs de filtre. Le tableau est trié par ordre alphabétique croissant par champ, puis par champ JSON.

Champ	Champ JSON	Description
ID de compte*	`accountId`	Identifiant unique de la personne Compte AWS à laquelle s'applique le résultat. Il s'agit généralement du compte propriétaire de la ressource affectée.
—	`archived`	Valeur booléenne qui indique si le résultat a été supprimé (archivé automatiquement) par une règle de suppression. Pour utiliser ce champ dans un filtre de la console, choisissez une option dans le menu État de recherche : Archivé (supprimé uniquemen

Champ	Champ JSON	Description
		t), En cours (non supprimé uniquement) ou Tout (supprimé et non supprimé).
Catégorie	`category`	Catégorie du résultat. La console fournit une liste de valeurs parmi lesquelle s choisir lorsque vous ajoutez ce champ à un filtre. Dans l'API, les valeurs valides sont :`CLASSIFIC ATION` , pour une recherche de données sensibles ; et`POLICY`, pour une constatat ion de politique.
—	`count`	Nombre total d'occurrences de la découverte. Pour les découvertes de données sensibles, cette valeur est toujours1. Toutes les données sensibles trouvées sont considérées comme uniques. Ce champ n'est pas disponibl e en tant qu'option de filtre sur la console. Avec l'API, vous pouvez utiliser ce champ pour définir une plage numérique pour un filtre.

Champ	Champ JSON	Description
Créé à	`createdAt`	Date et heure auxquelles Macie a créé le résultat. Vous pouvez utiliser ce champ pour définir une plage de temps pour un filtre.
Identifiant de recherche*	`id`	Identifiant unique de la recherche. Il s'agit d'une chaîne aléatoire que Macie génère et affecte à un résultat lorsqu'il crée le résultat.
Type de recherche*	`type`	Le type de résultat, par exemple, ou. `SensitiveData:S3Object/Personal` `Policy:IAMUser/S3BucketPublic` La console fournit une liste de valeurs parmi lesquelles choisir lorsque vous ajoutez ce champ à un filtre. Pour obtenir la liste des valeurs valides dans l'API, consultez le FindingTypemanuel Amazon Macie API Reference.
Région	`region`	Le dans Région AWS lequel Macie a créé le résultat, par exemple, ou. `us-east-1` `ca-central-1`

Champ	Champ JSON	Description
Exemple	`sample`	Valeur booléenne qui indique si le résultat est un exemple de résultat. Un exemple de résultat est un résultat qui utilise des données d'exemple et des valeurs d'espace réservé pour démontrer ce qu'un résultat peut contenir. La console fournit une liste de valeurs parmi lesquelles choisir lorsque vous ajoutez ce champ à un filtre.
Sévérité	`severity.description`	Représentation qualitative de la gravité du résultat. La console fournit une liste de valeurs parmi lesquelles choisir lorsque vous ajoutez ce champ à un filtre. Dans l'API, les valeurs valides sont : `Low`, `Medium`, et `High`.

Champ	Champ JSON	Description
Mis à jour le	`updatedAt`	Date et heure de la dernière mise à jour du résultat. Pour les résultats de données sensibles, cette valeur est identique à celle du champ Created at. Toutes les données sensibles découvert es sont considérées comme nouvelles (uniques). Vous pouvez utiliser ce champ pour définir une plage de temps pour un filtre.

* Pour spécifier plusieurs valeurs pour ce champ sur la console, ajoutez une condition qui utilise le champ et spécifie une valeur distincte pour le filtre, puis répétez cette étape pour chaque valeur supplémentaire. Pour ce faire avec l'API, utilisez un tableau répertoriant les valeurs à utiliser pour le filtre.

Champs de ressources concernés

Les rubriques suivantes répertorient et décrivent les champs que vous pouvez utiliser pour filtrer les résultats en fonction de la ressource à laquelle ils s'appliquent. Les sujets sont organisés par type de ressource.

Rubriques

- Compartiment S3
- Objet S3

Compartiment S3

Le tableau suivant répertorie et décrit les champs que vous pouvez utiliser pour filtrer les résultats en fonction des caractéristiques du compartiment S3 auquel s'applique un résultat.

Dans le tableau, la colonne Champ indique le nom du champ sur la console Amazon Macie. La colonne de champ JSON utilise la notation par points pour indiquer le nom du champ dans les représentations JSON des résultats et dans l'API Amazon Macie. (Les noms de champs JSON plus longs utilisent la nouvelle séquence de caractères (\n) pour améliorer la lisibilité.) La colonne Description fournit une brève description des données stockées dans le champ et indique les exigences relatives aux valeurs de filtre. Le tableau est trié par ordre alphabétique croissant par champ, puis par champ JSON.

Champ	Champ JSON	Description
—	`resourcesAffected.s3Bucket.createdAt`	La date et l'heure de création du compartiment concerné, ou les dernières modificat ions, telles que les modificat ions apportées à la politique du compartiment, ont été apportées au compartiment concerné. Ce champ n'est pas disponibl e en tant qu'option de filtre sur la console. Avec l'API, vous pouvez utiliser ce champ pour définir une plage de temps pour un filtre.
Chiffrement par défaut du compartiment S3	`resourcesAffected.s3Bucket.defaultServerSideEncryption.encryptionType`	Algorithme de chiffrement côté serveur utilisé par défaut pour chiffrer les objets ajoutés au compartiment concerné. La console fournit une liste de valeurs parmi lesquelles choisir lorsque vous ajoutez ce champ à un filtre. Pour obtenir la liste des valeurs

Champ	Champ JSON	Description
		valides pour l'API, consultez le EncryptionTypemanuel Amazon Macie API Reference.
ID de clé KMS de chiffrement du compartiment S3*	`resourcesAffected.s3Bucket.defaultServerSideEncryption.kmsMasterKeyId`	Le nom de ressource Amazon (ARN) ou l'AWS KMS keyidentifiant unique (ID clé) utilisé par défaut pour chiffrer les objets ajoutés au compartiment concerné.
Chiffrement du compartiment S3 requis par la politique du compartiment	`resourcesAffected.s3Bucket.allowsUnencryptedObjectUploads`	Spécifie si la politique de compartiment pour le compartiment concerné exige le chiffrement des objets côté serveur lorsque des objets sont ajoutés au compartiment. La console fournit une liste de valeurs parmi lesquelles choisir lorsque vous ajoutez ce champ à un filtre. Pour obtenir la liste des valeurs valides pour l'API, consultez S3Bucket dans le manuel Amazon Macie API Reference.
Nom du compartiment S3*	`resourcesAffected.s3Bucket.name`	Nom complet du compartiment concerné.
Nom d'affichage du propriétaire du compartiment S3*	`resourcesAffected.s3Bucket.owner.displayName`	Nom d'affichage de l'AWSutilisateur propriétaire du bucket concerné.

Champ	Champ JSON	Description
Autorisation d'accès public au compartiment S3	`resourcesAffected.s3Bucket.publicAccess.effectivePermission`	Spécifie si le compartiment concerné est accessible au public en fonction d'une combinaison de paramètres d'autorisation qui s'appliquent au compartiment. La console fournit une liste de valeurs parmi lesquelles choisir lorsque vous ajoutez ce champ à un filtre. Pour obtenir la liste des valeurs valides pour l'API, consultez le BucketPublicAccessmanuel Amazon Macie API Reference.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`accountLevelPermissions.blockPublicAccess.blockPublicAcls`
		Valeur booléenne qui indique si Amazon S3 bloque les listes de contrôle d'accès public (ACL) pour le compartiment concerné et les objets du compartiment. Il s'agit d'un paramètre de blocage de l'accès public au niveau du compte pour le bucket.
		
		Ce champ n'est pas disponible en tant qu'option de filtre sur la console.

Champ	Champ JSON	Description

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`accountLevelPermissions.blockPublicAccess.blockPublicPolicy`
		Valeur booléenne qui indique si Amazon S3 bloque les politiques de compartiment public pour le compartiment concerné. Il s'agit d'un paramètre de blocage de l'accès public au niveau du compte pour le bucket.
		
		Ce champ n'est pas disponible en tant qu'option de filtre sur la console.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`accountLevelPermissions.blockPublicAccess.ignorePublicAcls`
		Valeur booléenne qui indique si Amazon S3 ignore les ACL publiques pour le compartiment concerné et les objets du compartiment. Il s'agit d'un paramètre de blocage de l'accès public au niveau du compte pour le bucket.
		
		Ce champ n'est pas disponible en tant qu'option de filtre sur la console.

Champ	Champ JSON	Description
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n accountLevelPermissions.blockPublicAccess.restrictPublicBuckets`	Valeur booléenne qui indique si Amazon S3 restreint les politiques relatives aux compartiments publics pour le compartiment concerné. Il s'agit d'un paramètre de blocage de l'accès public au niveau du compte pour le bucket. Ce champ n'est pas disponible en tant qu'option de filtre sur la console.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.accessControlList.allowsPublicReadAccess`	Valeur booléenne qui indique si l'ACL au niveau du compartiment concerné accorde au grand public des autorisations d'accès en lecture pour le compartiment. Ce champ n'est pas disponible en tant qu'option de filtre sur la console.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.accessControlList.allowsPublicWriteAccess`	Valeur booléenne qui indique si l'ACL au niveau du compartiment concerné accorde au grand public des autorisations d'accès en écriture pour le compartiment. Ce champ n'est pas disponible en tant qu'option de filtre sur la console.

Champ	Champ JSON	Description

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.blockPublicAccess.blockPublicAcls`
		Valeur booléenne qui indique si Amazon S3 bloque les ACL publiques pour le compartiment concerné et les objets du compartiment. Il s'agit d'un paramètre de blocage de l'accès public au niveau du compartiment pour un compartiment.
		
		Ce champ n'est pas disponible en tant qu'option de filtre sur la console.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.blockPublicAccess.blockPublicPolicy`
		Valeur booléenne qui indique si Amazon S3 bloque les politiques de compartiment public pour le compartiment concerné. Il s'agit d'un paramètre d'accès public bloqué au niveau du compartiment pour le compartiment.
		
		Ce champ n'est pas disponible en tant qu'option de filtre sur la console.

Champ	Champ JSON	Description

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.blockPublicAccess.ignorePublicAcls`
		Valeur booléenne qui indique si Amazon S3 ignore les ACL publiques pour le compartiment concerné et les objets du compartiment. Il s'agit d'un paramètre d'accès public bloqué au niveau du compartiment pour le compartiment.
		
		Ce champ n'est pas disponible en tant qu'option de filtre sur la console.

—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n`
	
	`bucketLevelPermissions.blockPublicAccess.restrictPublicBuckets`
		Valeur booléenne qui indique si Amazon S3 restreint les politiques relatives aux compartiments publics pour le compartiment concerné. Il s'agit d'un paramètre d'accès public bloqué au niveau du compartiment pour le compartiment.
		
		Ce champ n'est pas disponible en tant qu'option de filtre sur la console.

Champ	Champ JSON	Description
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.bucketPolicy.allowsPublicReadAccess`	Valeur booléenne qui indique si la politique du bucket concerné autorise le grand public à avoir un accès en lecture au bucket. Ce champ n'est pas disponible en tant qu'option de filtre sur la console.
—	`resourcesAffected.s3Bucket.publicAccess.permissionConfiguration.\n bucketLevelPermissions.bucketPolicy.allowsPublicWriteAccess`	Valeur booléenne qui indique si la politique du bucket concerné autorise le grand public à avoir un accès en écriture au bucket. Ce champ n'est pas disponible en tant qu'option de filtre sur la console.
Clé d'identification du compartiment S3*	`resourcesAffected.s3Bucket.tags.key`	Une clé de balise associée au compartiment concerné.
Valeur de l'étiquette du compartiment S3*	`resourcesAffected.s3Bucket.tags.value`	Une valeur de balise associée au compartiment concerné.

* Pour spécifier plusieurs valeurs pour ce champ sur la console, ajoutez une condition qui utilise le champ et spécifie une valeur distincte pour le filtre, puis répétez cette étape pour chaque valeur supplémentaire. Pour ce faire avec l'API, utilisez un tableau répertoriant les valeurs à utiliser pour le filtre.

Objet S3

Le tableau suivant répertorie et décrit les champs que vous pouvez utiliser pour filtrer les résultats en fonction des caractéristiques de l'objet S3 auquel s'applique un résultat.

Dans le tableau, la colonne Champ indique le nom du champ sur la console Amazon Macie. La colonne de champ JSON utilise la notation par points pour indiquer le nom du champ dans les représentations JSON des résultats et dans l'API Amazon Macie. La colonne Description fournit une brève description des données stockées dans le champ et indique les exigences relatives aux valeurs de filtre. Le tableau est trié par ordre alphabétique croissant par champ, puis par champ JSON.

Champ	Champ JSON	Description
ID de clé KMS de chiffrement des objets S3*	`resourcesAffected.s3Object.serverSideEncryption.kmsMasterKeyId`	Le nom de ressource Amazon (ARN) ou l'identifiant unique (ID clé) utilisé pour chiffrer l'objet concerné. AWS KMS key
Type de chiffrement d'objet S3	`resourcesAffected.s3Object.serverSideEncryption.encryptionType`	Algorithme de chiffrement côté serveur qui a été utilisé pour chiffrer l'objet concerné. La console fournit une liste de valeurs parmi lesquelles choisir lorsque vous ajoutez ce champ à un filtre. Pour obtenir la liste des valeurs valides pour l'API, consultez le EncryptionTypemanuel Amazon Macie API Reference.
—	`resourcesAffected.s3Object.extension`	L'extension du nom de fichier de l'objet concerné. Pour les objets qui n'ont pas d'extensi on de nom de fichier, spécifiez "" la valeur du filtre. Ce champ n'est pas disponible en tant qu'option de filtre sur la console.

Champ	Champ JSON	Description
—	`resourcesAffected.s3Object.lastModified`	Date et heure de création ou de dernière modification de l'objet concerné, selon la date la plus récente. Ce champ n'est pas disponible en tant qu'option de filtre sur la console. Avec l'API, vous pouvez utiliser ce champ pour définir une plage de temps pour un filtre.
Clé d'objet S3*	`resourcesAffected.s3Object.key`	Le nom complet (clé) de l'objet concerné, y compris le préfixe de l'objet le cas échéant.
—	`resourcesAffected.s3Object.path`	Le chemin complet vers l'objet concerné, y compris le nom du compartiment concerné et le nom de l'objet (clé). Ce champ n'est pas disponible en tant qu'option de filtre sur la console.

Champ	Champ JSON	Description
Accès public aux objets S3	`resourcesAffected.s3Object.publicAccess`	Valeur booléenne qui indique si l'objet concerné est accessible au public en fonction d'une combinaison de paramètres d'autorisation qui s'appliquent à l'objet. La console fournit une liste de valeurs parmi lesquelles choisir lorsque vous ajoutez ce champ à un filtre.
Clé de balise d'objet S3*	`resourcesAffected.s3Object.tags.key`	Une clé de balise associée à l'objet concerné.
Valeur de la balise d'objet S3*	`resourcesAffected.s3Object.tags.value`	Une valeur de balise associée à l'objet concerné.

* Pour spécifier plusieurs valeurs pour ce champ sur la console, ajoutez une condition qui utilise le champ et spécifie une valeur distincte pour le filtre, puis répétez cette étape pour chaque valeur supplémentaire. Pour ce faire avec l'API, utilisez un tableau répertoriant les valeurs à utiliser pour le filtre.

Champs de politique

Le tableau suivant répertorie et décrit les champs que vous pouvez utiliser pour filtrer les résultats des politiques. Ces champs stockent des données spécifiques aux conclusions des politiques.

Dans le tableau, la colonne Champ indique le nom du champ sur la console Amazon Macie. La colonne de champ JSON utilise la notation par points pour indiquer le nom du champ dans les représentations JSON des résultats et dans l'API Amazon Macie. (Les noms de champs JSON plus longs utilisent la nouvelle séquence de caractères (\n) pour améliorer la lisibilité.) La colonne Description fournit une brève description des données stockées dans le champ et indique les

exigences relatives aux valeurs de filtre. Le tableau est trié par ordre alphabétique croissant par champ, puis par champ JSON.

Champ	Champ JSON	Description
Type d'action	`policyDetails.action.actionType`	Type d'action à l'origine du résultat. La seule valeur valide pour ce champ est`AWS_API_CALL` .
Nom de l'appel de l'API*	`policyDetails.action.apiCallDetails.api`	Nom de l'opération qui a été invoquée le plus récemment et qui a produit le résultat, par exemple,. `PutBucketPublicAccessBlock`
Nom du service API*	`policyDetails.action.apiCallDetails.apiServiceName`	L'URL du Service AWS qui fournit l'opération qui a été invoquée et a produit le résultat, par exemple,. `s3.amazonaws.com`
—	`policyDetails.action.apiCallDetails.firstSeen`	Date et heure auxquelles une opération a été invoquée pour la première fois et a produit le résultat. Ce champ n'est pas disponible en tant qu'option de filtre sur la console. Avec l'API, vous pouvez utiliser ce champ pour définir une plage de temps pour un filtre.
—	`policyDetails.action.apiCallDetails.lastSeen`	Date et heure les plus récentes auxquelles l'opération spécifiée (nom de l'appel

Champ	Champ JSON	Description
		d'API ou`api`) a été invoquée et a produit le résultat. Ce champ n'est pas disponibl e en tant qu'option de filtre sur la console. Avec l'API, vous pouvez utiliser ce champ pour définir une plage de temps pour un filtre.
—	`policyDetails.acto r.domainDetails.do mainName`	Le nom de domaine de l'appareil qui a été utilisé pour effectuer l'action. Ce champ n'est pas disponible en tant qu'option de filtre sur la console.
Ville IP*	`policyDetails.acto r.ipAddressDetails .ipCity.name`	Nom de la ville d'origine de l'adresse IP de l'appareil utilisé pour effectuer l'action.
Pays IP*	`policyDetails.acto r.ipAddressDetails .ipCountry.name`	Le nom du pays d'origine de l'adresse IP de l'appareil utilisé pour effectuer l'action, par exemple,. `United States`
—	`policyDetails.acto r.ipAddressDetails .ipOwner.asn`	Numéro de système autonome (ASN) du système autonome qui incluait l'adresse IP de l'appareil utilisé pour effectuer l'action. Ce champ n'est pas disponible en tant qu'option de filtre sur la console.

Champ	Champ JSON	Description
Organisme ASN du propriétaire de l'IP *	`policyDetails.actor.ipAddressDetails.ipOwner.asnOrg`	Identifiant d'organisation associé à l'ASN du système autonome qui incluait l'adresse IP de l'appareil utilisé pour effectuer l'action.
ISP* propriétaire de l'IP	`policyDetails.actor.ipAddressDetails.ipOwner.isp`	Nom du fournisseur de services Internet (ISP) propriétaire de l'adresse IP de l'appareil utilisé pour effectuer l'action.
Adresse IP V4*	`policyDetails.actor.ipAddressDetails.ipAddressV4`	Adresse IPv4 (Internet Protocol version 4) de l'appareil utilisé pour effectuer l'action.
—	`policyDetails.actor.userIdentity.assumedRole.accessKeyId`	Pour une action effectuée avec des informations d'identification de sécurité temporaires obtenues à l'aide `AssumeRole` de l'AWS STSAPI, l'ID de clé AWS d'accès identifiant les informations d'identification. Ce champ n'est pas disponible en tant qu'option de filtre sur la console.

Champ	Champ JSON	Description
Identité de l'utilisateur : rôle assumé, identifiant du compte*	`policyDetails.actor.userIdentity.assumedRole.accountId`	Pour une action effectuée avec des informations d'identification de sécurité temporaires obtenues à `AssumeRole` l'aide de l'AWS STSAPI, identifiant unique de l'Compte AWSentité propriétaire de l'entité utilisée pour obtenir les informations d'identification.
Identité de l'utilisateur : identifiant du rôle principal*	`policyDetails.actor.userIdentity.assumedRole.principalId`	Pour une action effectuée avec des informations d'identification de sécurité temporaires obtenues `AssumeRole` à l'aide de l'AWS STSAPI, identifiant unique de l'entité utilisée pour obtenir les informations d'identification.
Identité de l'utilisateur : rôle assumé, session, ARN*	`policyDetails.actor.userIdentity.assumedRole.arn`	Pour une action effectuée avec des informations d'identification de sécurité temporaires obtenues à l'`AssumeRole` aide de l'AWS STSAPI, l'Amazon Resource Name (ARN) du compte source, de l'utilisateur IAM ou du rôle utilisé pour obtenir les informations d'identification.

Champ	Champ JSON	Description
—	`policyDetails.actor.userIdentity.assumedRole.sessionContext.\n sessionIssuer.type`	Pour une action effectuée avec des informations d'identification de sécurité temporaires obtenues `AssumeRole` à l'aide de l'AWS STSAPI, la source des informations de sécurité temporaires, par exemple `RootIAMUser`, ou`Role`. Ce champ n'est pas disponible en tant qu'option de filtre sur la console.
—	`policyDetails.actor.userIdentity.assumedRole.sessionContext.\n sessionIssuer.userName`	Pour une action effectuée avec des informations de sécurité temporaires obtenues à l'aide `AssumeRole` de l'AWS STSAPI, le nom ou l'alias de l'utilisateur ou du rôle qui a émis la session. Notez que cette valeur est nulle si les informations d'identification ont été obtenues à partir d'un compte racine qui n'a pas d'alias. Ce champ n'est pas disponible en tant qu'option de filtre sur la console.

Champ	Champ JSON	Description
Identité d'utilisateur AWS Identifiant du compte*	`policyDetails.actor.userIdentity.awsAccount.accountId`	Pour une action effectuée à l'aide des informations d'identification d'une autre personneCompte AWS, l'identifiant unique du compte.
Identité de l'utilisateur : AWS identifiant principal du compte*	`policyDetails.actor.userIdentity.awsAccount.principalId`	Pour une action exécutée à l'aide des informations d'identification d'une autreCompte AWS, identifiant unique de l'entité qui a effectué l'action.
AWSService d'identité utilisateur invoqué par	`policyDetails.actor.userIdentity.awsService.invokedBy`	Pour une action effectuée par un compte appartenant à unService AWS, le nom du service.
—	`policyDetails.actor.userIdentity.federatedUser.accessKeyId`	Pour une action effectuée avec des informations d'identification de sécurité temporaires obtenues à l'aide `GetFederationToken` de l'AWS STSAPI, l'ID de clé AWS d'accès identifiant les informations d'identification. Ce champ n'est pas disponible en tant qu'option de filtre sur la console.

Champ	Champ JSON	Description
Session fédérée d'identité utilisateur ARN*	`policyDetails.actor.userIdentity.federatedUser.arn`	Pour une action effectuée avec des informations d'identification de sécurité temporaires obtenues à `GetFederationToken` l'aide de l'AWS STSAPI, l'ARN de l'entité utilisée pour obtenir les informations d'identification.
Identité de l'utilisateur Identifiant du compte utilisateur fédéré *	`policyDetails.actor.userIdentity.federatedUser.accountId`	Pour une action effectuée avec des informations d'identification de sécurité temporaires obtenues à `GetFederationToken` l'aide de l'AWS STSAPI, identifiant unique de l'Compte AWSentité propriétaire de l'entité utilisée pour obtenir les informations d'identification.
Identité de l'utilisateur : identifiant d'utilisateur principal fédéré *	`policyDetails.actor.userIdentity.federatedUser.principalId`	Pour une action effectuée avec des informations d'identification de sécurité temporaires obtenues `GetFederationToken` à l'aide de l'AWS STSAPI, identifiant unique de l'entité utilisée pour obtenir les informations d'identification.

Champ	Champ JSON	Description
—	`policyDetails.actor.userIdentity.federatedUser.sessionContext.\n sessionIssuer.type`	Pour une action effectuée avec des informations d'identification de sécurité temporaires obtenues à `GetFederationToken` l'aide de l'AWS STSAPI, la source des informations de sécurité temporaires, par exemple`Root`, `IAMUser` ou. `Role` Ce champ n'est pas disponible en tant qu'option de filtre sur la console.
—	`policyDetails.actor.userIdentity.federatedUser.sessionContext.\n sessionIssuer.userName`	Pour une action effectuée avec des informations de sécurité temporaires obtenues à l'aide `GetFederationToken` de l'AWS STSAPI, le nom ou l'alias de l'utilisateur ou du rôle qui a émis la session. Notez que cette valeur est nulle si les informations d'identification ont été obtenues à partir d'un compte racine qui n'a pas d'alias. Ce champ n'est pas disponible en tant qu'option de filtre sur la console.

Champ	Champ JSON	Description
Identité de l'utilisateur Identifiant du compte IAM*	`policyDetails.actor.userIdentity.iamUser.accountId`	Pour une action effectuée à l'aide des informations d'identification d'un utilisateur IAM, l'Compte AWSidentifiant unique associé à l'utilisateur IAM qui a effectué l'action.
Identité de l'utilisateur ID principal IAM*	`policyDetails.actor.userIdentity.iamUser.principalId`	Pour une action effectuée à l'aide des informations d'identification d'un utilisateur IAM, identifiant unique de l'utilisateur IAM qui a effectué l'action.
Identité utilisateur Nom d'utilisateur IAM*	`policyDetails.actor.userIdentity.iamUser.userName`	Pour une action effectuée à l'aide des informations d'identification d'un utilisateur IAM, nom d'utilisateur de l'utilisateur IAM qui a effectué l'action.
Identité de l'utilisateur Identifiant du compte root *	`policyDetails.actor.userIdentity.root.accountId`	Pour une action effectuée à l'aide des informations d'identification de votre compteCompte AWS, l'identifiant unique du compte.
Identité de l'utilisateur : identifiant principal root *	`policyDetails.actor.userIdentity.root.principalId`	Pour une action effectuée à l'aide des informations d'identification de votreCompte AWS, l'identifiant unique de l'entité qui a effectué l'action.

Champ	Champ JSON	Description
Type d'identité de l'utilisateur	`policyDetails.actor.userIdentity.type`	Type d'entité ayant effectué l'action à l'origine du résultat. La console fournit une liste de valeurs parmi lesquelles choisir lorsque vous ajoutez ce champ à un filtre. Pour obtenir la liste des valeurs valides pour l'API, consultez le UserIdentityTypemanuel Amazon Macie API Reference.

* Pour spécifier plusieurs valeurs pour ce champ sur la console, ajoutez une condition qui utilise le champ et spécifie une valeur distincte pour le filtre, puis répétez cette étape pour chaque valeur supplémentaire. Pour ce faire avec l'API, utilisez un tableau répertoriant les valeurs à utiliser pour le filtre.

Champs de classification des données sensibles

Le tableau suivant répertorie et décrit les champs que vous pouvez utiliser pour filtrer les résultats de données sensibles. Ces champs stockent des données spécifiques aux résultats de données sensibles.

Dans le tableau, la colonne Champ indique le nom du champ sur la console Amazon Macie. La colonne de champ JSON utilise la notation par points pour indiquer le nom du champ dans les représentations JSON des résultats et dans l'API Amazon Macie. La colonne Description fournit une brève description des données stockées dans le champ et indique les exigences relatives aux valeurs de filtre. Le tableau est trié par ordre alphabétique croissant par champ, puis par champ JSON.

Champ	Champ JSON	Description
ID d'identifiant de données personnalisé*	`classificationDetails.result.customDataIdentifiers.detections.arn`	Identifiant unique de l'identifiant de données personnalisé

Champ	Champ JSON	Description
		qui a détecté les données et produit le résultat.
Nom de l'identifiant de données personnalisé*	`classificationDetails.result.customDataIdentifiers.detections.name`	Nom de l'identifiant de données personnalisé qui a détecté les données et produit le résultat.
Nombre total d'identifiants de données personnalisés	`classificationDetails.result.customDataIdentifiers.detections.count`	Nombre total d'occurrences de données détectées par des identifiants de données personnalisés et à l'origine du résultat. Vous pouvez utiliser ce champ pour définir une plage numérique pour un filtre.
Numéro du poste*	`classificationDetails.jobId`	Identifiant unique de la tâche de découverte de données sensibles à l'origine de la découverte.
Type d'origine	`classificationDetails.originType`	Comment Macie a trouvé les données sensibles à l'origine de la découverte : `AUTOMATED_SENSITIVE_DATA_DISCOVERY` ou `SENSITIVE_DATA_DISCOVERY_JOB` .

Champ	Champ JSON	Description
—	`classificationDetails.result.mimeType`	Type de contenu, en tant que type MIME, auquel le résultat s'applique, par exemple, pour un fichier CSV ou `text/csv` `application/pdf` pour un fichier Adobe Portable Document Format. Ce champ n'est pas disponible en tant qu'option de filtre sur la console.
—	`classificationDetails.result.sizeClassified`	Taille de stockage totale, en octets, de l'objet S3 auquel le résultat s'applique. Ce champ n'est pas disponible en tant qu'option de filtre sur la console. Avec l'API, vous pouvez utiliser ce champ pour définir une plage numérique pour un filtre.

Champ	Champ JSON	Description
Code d'état du résultat*	`classificationDetails.result.status.code`	État de la découverte. Les valeurs valides sont : • `COMPLETE`— Macie a terminé son analyse de l'objet. • `PARTIAL`— Macie n'a analysé qu'un sous-ensemble des données de l'objet. Par exemple, l'objet est un fichier d'archive contenant des fichiers dans un format non pris en charge. • `SKIPPED`— Macie n'a pas pu analyser l'objet. Par exemple, l'objet est un fichier mal formé.
Catégorie de données sensibles	`classificationDetails.result.sensitiveData.category`	Catégorie de données sensibles détectées et à l'origine du résultat. La console fournit une liste de valeurs parmi lesquelles s choisir lorsque vous ajoutez ce champ à un filtre. Dans l'API, les valeurs valides sont : `CREDENTIALS FINANCIAL_INFORMATION` , et`PERSONAL_INFORMATION` .

Champ	Champ JSON	Description
Type de détection de données sensibles	`classificationDetails.result.sensitiveData.detections.type`	Type de données sensibles détectées et à l'origine du résultat. La console fournit une liste de valeurs parmi lesquelles choisir lorsque vous ajoutez ce champ à un filtre. Pour obtenir la liste des valeurs valides pour la console et pour l'API, consultezTypes de détection de données sensibles.
Nombre total de données sensibles	`classificationDetails.result.sensitiveData.detections.count`	Nombre total d'occurrences des données sensibles détectées et à l'origine du résultat. Vous pouvez utiliser ce champ pour définir une plage numérique pour un filtre.

* Pour spécifier plusieurs valeurs pour ce champ sur la console, ajoutez une condition qui utilise le champ et spécifie une valeur distincte pour le filtre, puis répétez cette étape pour chaque valeur supplémentaire. Pour ce faire avec l'API, utilisez un tableau répertoriant les valeurs à utiliser pour le filtre.

Types de détection de données sensibles

Les rubriques suivantes répertorient les valeurs que vous pouvez spécifier pour le champ Type de détection de données sensibles dans un filtre. (Le nom JSON de ce champ est`classificationDetails.result.sensitiveData.detections.type`.) Les sujets sont organisés en fonction des catégories de données sensibles que Macie peut détecter à l'aide d'identifiants de données gérés.

Catégories

- Informations d'identification
- Informations financières
- Informations personnelles : Informations médicales personnelles (PHI)
- Informations personnelles : informations personnelles identifiables (PII)

Pour en savoir plus sur l'identifiant de données gérées pour un type spécifique de données sensibles, consultezRéférence détaillée : Identifiants de données gérés par Amazon Macie.

Informations d'identification

Vous pouvez spécifier les valeurs suivantes pour filtrer les résultats qui signalent des occurrences de données d'identification dans des objets S3.

Type de données sensibles	Valeur du filtre
Clé d'accès secrète AWS	`AWS_CREDENTIALS`
Clé d'API Google Cloud	`GCP_API_KEY`
En-tête d'autorisation HTTP Basic	`HTTP_BASIC_AUTH_HEADER`
Jeton Web JSON (JWT)	`JSON_WEB_TOKEN`
Clé privée OpenSSH	`OPENSSH_PRIVATE_KEY`
Clé privée PGP	`PGP_PRIVATE_KEY`
Clé privée selon la norme PKCS (Public Key Cryptography Standard)	`PKCS`
Clé privée PuTTY	`PUTTY_PRIVATE_KEY`
Clé d'API Stripe	`STRIPE_CREDENTIALS`

Informations financières

Vous pouvez spécifier les valeurs suivantes pour filtrer les résultats qui signalent des occurrences d'informations financières dans des objets S3.

Type de données sensibles	Valeur du filtre
Numéro de compte bancaire	`BANK_ACCOUNT_NUMBER` (pour le Canada et les États-Unis)
Numéro de compte bancaire de base (BBAN)	En fonction du pays ou de la région : `FRANCE_BANK_ACCOUNT_NUMBER`, `GERMANY_BANK_ACCOUNT_NUMBER`, `ITALY_BANK_ACCOUNT_NUMBER`, `SPAIN_BANK_ACCOUNT_NUMBER`, `UK_BANK_ACCOUNT_NUMBER`
Date d'expiration de carte de crédit	`CREDIT_CARD_EXPIRATION`
Données relatives à la bande magnétique des cartes de crédit	`CREDIT_CARD_MAGNETIC_STRIPE`
Numéro de carte de crédit	`CREDIT_CARD_NUMBER` (pour les numéros de carte de crédit situés à proximité d'un mot clé), `CREDIT_CARD_NUMBER_(NO_KEYWORD)` (pour les numéros de carte de crédit situés à proximité d'un mot clé)
Code de vérification de carte de crédit	`CREDIT_CARD_SECURITY_CODE`
Numéro de compte bancaire international (IBAN)	Selon le pays ou la région : `ALBANIA_BANK_ACCOUNT_NUMBER`, `ANDORRA_BANK_ACCOUNT_NUMBER`, `BOSNIA_AND_HERZEGOVINA_BANK_ACCOUNT_NUMBER`, `BRAZIL_BANK_ACCOUNT_NUMBER`, `BULGARIA_BANK_ACCOUNT_NUMBER`, `COSTA_RICA_BANK_ACCOUNT_NUMBER`, `CROATIA_BANK_ACCOUNT_NUMBER`, `CYPRUS_BANK_ACCOUNT_NUMBER`, `CZECH_REPUBLIC_BANK_ACCOUNT_NUMBER`, `DENMARK_BANK_ACCOUNT_NUMBER`, `DOMINICAN`

Type de données sensibles	Valeur du filtre
	_REPUBLIC_BANK_ACCOUNT_NUMB ER, EGYPT_BANK_ACCOUNT_NUM BER, ESTONIA_BANK_ACCOUNT_NUMBER , FAROE_ISLANDS_BANK_ACCOU NT_NUMBER, FINLAND_BANK_AC COUNT_NUMBER, FRANCE_BANK_ACCOUN T_NUMBER, GEORGIA_BANK_ACC OUNT_NUMBER, GERMANY_BANK_ACCOU NT_NUMBER, GREECE_BANK_ACC OUNT_NUMBER, GREENLAND_BANK_ACC OUNT_NUMBER, HUNGARY_BANK_ ACCOUNT_NUMBER, ICELAND_B ANK_ACCOUNT_NUMBER, IRELAN D_BANK_ACCOUNT_NUMBER, ITALY_BAN K_ACCOUNT_NUMBER, JORDAN_B ANK_ACCOUNT_NUMBER, KOSOVO_BA NK_ACCOUNT_NUMBER, LIECHTE NSTEIN_BANK_ACCOUNT_NUMBER, LITHUANIA_BANK_ACCOUNT_NUMBER, MALTA_BANK_ACCOUNT_NUMBER, MAURITANIA_BANK_ACCOUNT_NUMBER, MAURITIUS_BANK_ACCOUNT_NUMBER , MONACO_BANK_ACCOUNT_NUMBER, MONTENEGRO_BANK_ACCOUNT_N UMBER, NETHERLANDS_BANK_AC COUNT_NUMBER, NORTH_MACEDO NIA_BANK_ACCOUNT_NUMBER, P OLAND_BANK_ACCOUNT_NUMBER, PORTUGAL_BANK_ACCOUNT_NUMBER, SAN_MARINO_BANK_ACCOUNT_NUMBER, SENEGAL_BANK_ACCOUNT_NUMBER, SERBIA_BANK_ACCOUNT_NUMBER, SLOVAKIA_BANK_ACCOUNT_NUMBER, SLOVENIA_BANK_ACCOUNT_NUMBER,

Type de données sensibles	Valeur du filtre
	`SPAIN_BANK_ACCOUNT_NUMBER, SWEDEN_BANK_ACCOUNT_NUMBER, SWITZERLAND_BANK_ACCOUNT_NUMBER, TIMOR_LESTE_BANK_ACCOUNT_NUMBER, TUNISIA_BANK_ACCOUNT_NUMBER, TURKIYE_BANK_ACCOUNT_NUMBER, UK_BANK_ACCOUNT_NUMBER, UKRAINE_BANK_ACCOUNT_NUMBER, UNITED_ARAB_EMIRATES_BANK_ACCOUNT_NUMBER, VIRGIN_ISLANDS_BANK_ACCOUNT_NUMBER` (pour les îles Vierges britanniques)

Informations personnelles : Informations médicales personnelles (PHI)

Vous pouvez spécifier les valeurs suivantes pour filtrer les résultats signalant des occurrences d'informations médicales personnelles (PHI) dans des objets S3.

Type de données sensibles	Valeur du filtre
Numéro d'enregistrement de la Drug Enforcement Agency (DEA)	`US_DRUG_ENFORCEMENT_AGENCY_NUMBER`
Numéro de réclamation d'assurance maladie (HICN)	`USA_HEALTH_INSURANCE_CLAIM_NUMBER`
Numéro d'assurance maladie ou d'identification médicale	En fonction du pays ou de la région : `CANADA_HEALTH_NUMBER, EUROPEAN_HEALTH_INSURANCE_CARD_NUMBER, FINLAND_EUROPEAN_HEALTH_INSURANCE_NUMBER, FRANCE_HEALTH_INSURANCE_NUMBER, UK_NHS_NUMBER, USA_MEDICARE_BENEFICIARY_IDENTIFIER`

Type de données sensibles	Valeur du filtre
Code du système de codage des procédures communes pour les soins de santé (HCPCS)	`USA_HEALTHCARE_PROCEDURE_CODE`
Code national des médicaments (NDC)	`USA_NATIONAL_DRUG_CODE`
Identifiant national du fournisseur (NPI)	`USA_NATIONAL_PROVIDER_IDENTIFIER`
Identifiant unique de l'appareil (UDI)	`MEDICAL_DEVICE_UDI`

Informations personnelles : informations personnelles identifiables (PII)

Vous pouvez spécifier les valeurs suivantes pour filtrer les résultats qui signalent des occurrences d'informations personnelles identifiables (PII) dans les objets S3.

Type de données sensibles	Valeur du filtre
Date de naissance	`DATE_OF_BIRTH`
Numéro d'identification du permis de conduire	Selon le pays ou la région : `AUSTRALIA_DRIVERS_LICENSE`, `AUSTRIA_DRIVERS_LICENSE`, `BELGIUM_DRIVERS_LICENSE`, `BULGARIA_DRIVERS_LICENSE`, `CANADA_DRIVERS_LICENSE`, `CROATIA_DRIVERS_LICENSE`, `CYPRUS_DRIVERS_LICENSE`, `CZECHIA_DRIVERS_LICENSE`, `DENMARK_DRIVERS_LICENSE`, `DRIVERS_LICENSE` (pour les États-Unis), `ESTONIA_DRIVERS_LICENSE`, `FINLAND_DRIVERS_LICENSE`, `FRANCE_DRIVERS_LICENSE`, `GERMANY_DRIVERS_LICENSE`, `GREECE_DRIVERS_LICENSE`, `HUNGARY_DRIVERS_LICENSE`, `INDIA_DRIVERS_LICENSE`, `IRELAND_DRIVERS_LI`

Type de données sensibles	Valeur du filtre
	CENSE, ITALY_DRIVERS_LICEN SE, LATVIA_DRIVERS_LICENSE, LITHUANIA_DRIVERS_LICENSE, LUXEMBOURG_DRIVERS_LICENSE, MALTA_DRIVERS_LICENSE, NETHERLAN DS_DRIVERS_LICENSE, POLAND _DRIVERS_LICENSE, PORTUGAL_ DRIVERS_LICENSE, ROMANIA_D RIVERS_LICENSE, SLOVAKIA_ DRIVERS_LICENSE, SLOVENIA_ DRIVERS_LICENSE, SPAIN_DRI VERS_LICENSE, SWEDEN_DRIVE RS_LICENSE, UK_DRIVERS_LICENSE
Numéro de liste électorale	UK_ELECTORAL_ROLL_NUMBER
Nom complet	NAME
Coordonnées du système de positionnement global (GPS)	LATITUDE_LONGITUDE
Cookie HTTP	HTTP_COOKIE
Adresse postale	ADDRESS, BRAZIL_CEP_CODE
Numéro d'identification nationale	En fonction du pays ou de la région : BRAZIL_RG_NUMBER, FRANCE_N ATIONAL_IDENTIFICATION_NUMB ER, GERMANY_NATIONAL_IDENT IFICATION_NUMBER, INDIA_AA DHAAR_NUMBER, ITALY_NATIONAL_IDE NTIFICATION_NUMBER, SPAIN_ DNI_NUMBER
Numéro d'assurance nationale (NINO)	UK_NATIONAL_INSURANCE_NUMBER

Type de données sensibles	Valeur du filtre
Numéro de passeport	En fonction du pays ou de la région : `CANADA_PASSPORT_NUMBER`, `FRANCE_PASSPORT_NUMBER`, `GERMANY_PASSPORT_NUMBER`, `ITALY_PASSPORT_NUMBER`, `SPAIN_PASSPORT_NUMBER`, `UK_PASSPORT_NUMBER`, `USA_PASSPORT_NUMBER`
Numéro de résidence permanente	`CANADA_NATIONAL_IDENTIFICATION_NUMBER`
Phone number (Numéro de téléphone)	Selon le pays ou la région : `BRAZIL_PHONE_NUMBER`, `FRANCE_PHONE_NUMBER`, `GERMANY_PHONE_NUMBER`, `ITALY_PHONE_NUMBER`, `PHONE_NUMBER` (pour le Canada et les États-Unis), `SPAIN_PHONE_NUMBER`, `UK_PHONE_NUMBER`
Numéro d'assurance sociale (SIN)	`CANADA_SOCIAL_INSURANCE_NUMBER`
Numéro de sécurité sociale (SSN)	En fonction du pays ou de la région : `SPAIN_SOCIAL_SECURITY_NUMBER`, `USA_SOCIAL_SECURITY_NUMBER`

Type de données sensibles	Valeur du filtre
Numéro d'identification ou de référence du contribuable	En fonction du pays ou de la région : `AUSTRALIA_TAX_FILE_NUMBER, BRAZIL_CNPJ_NUMBER, BRAZIL_CPF_NUMBER, FRANCE_TAX_IDENTIFICATION_NUMBER, GERMANY_TAX_IDENTIFICATION_NUMBER, INDIA_PERMANENT_ACCOUNT_NUMBER, SPAIN_NIE_NUMBER, SPAIN_NIF_NUMBER, SPAIN_TAX_IDENTIFICATION_NUMBER, UK_TAX_IDENTIFICATION_NUMBER, USA_INDIVIDUAL_TAX_IDENTIFICATION_NUMBER`
Numéro d'identification du véhicule (VIN)	`VEHICLE_IDENTIFICATION_NUMBER`

Examiner des données sensibles à l'aide des résultats d'Amazon Macie

Lorsque vous exécutez des tâches de découverte de données sensibles ou qu'Amazon Macie effectue une découverte automatique de données sensibles, Macie collecte des informations sur l'emplacement de chaque occurrence de données sensibles qu'elle trouve dans les objets Amazon Simple Storage Service (Amazon S3). Cela inclut les données sensibles détectées par Macie à l'aide d'identifiants de données gérés, ainsi que les données qui répondent aux critères des identifiants de données personnalisés que vous configurez une tâche ou que Macie utilisera.

Avec les résultats de données sensibles, vous pouvez consulter ces informations pour jusqu'à 15 occurrences de données sensibles que Macie trouve dans des objets S3 individuels. Les détails donnent un aperçu de l'étendue des catégories et des types de données sensibles que des compartiments et objets S3 spécifiques peuvent contenir. Ils peuvent vous aider à localiser des occurrences individuelles de données sensibles dans des objets et à déterminer s'il convient d'effectuer une enquête plus approfondie sur des compartiments et des objets spécifiques.

Pour plus d'informations, vous pouvez éventuellement configurer et utiliser Macie pour récupérer des échantillons de données sensibles que Macie rapporte dans des résultats individuels. Les exemples peuvent vous aider à vérifier la nature des données sensibles découvertes par Macie. Ils peuvent également vous aider à personnaliser votre enquête sur un compartiment et un objet S3 concernés. Si vous choisissez de récupérer des échantillons de données sensibles pour un résultat, Macie utilise les données du résultat pour localiser 1 à 10 occurrences de chaque type de données sensibles signalé par le résultat. Macie extrait ensuite ces occurrences de données sensibles de l'objet concerné et affiche les données pour que vous puissiez les consulter.

Si un objet S3 contient de nombreuses occurrences de données sensibles, une découverte peut également vous aider à accéder au résultat de découverte de données sensibles correspondant. Contrairement à la découverte de données sensibles, un résultat de découverte de données sensibles fournit des données de localisation détaillées pour jusqu'à 1 000 occurrences de chaque type de données sensibles que Macie trouve dans un objet. Macie utilise le même schéma pour les données de localisation dans les résultats de recherche de données sensibles et les résultats de découverte de données sensibles. Pour en savoir plus sur les résultats de découverte de données sensibles, consultezStockage et conservation des résultats de découverte de données sensibles.

Les rubriques de cette section expliquent comment localiser et éventuellement récupérer les occurrences de données sensibles signalées par des découvertes de données sensibles. Ils expliquent également le schéma utilisé par Macie pour signaler l'emplacement des occurrences individuelles de données sensibles détectées par Macie.

Rubriques

- Localisation de données sensibles grâce aux résultats d'Amazon Macie
- Extraction d'échantillons de données sensibles grâce aux résultats d'Amazon Macie
- Schéma JSON pour les emplacements de données sensibles

Localisation de données sensibles grâce aux résultats d'Amazon Macie

Lorsque vous exécutez des tâches de découverte de données sensibles ou qu'Amazon Macie effectue une découverte automatique de données sensibles, Macie effectue une inspection approfondie de la dernière version de chaque objet Amazon Simple Storage Service (Amazon S3) qu'il analyse. Pour chaque exécution de tâche ou cycle d'analyse, Macie utilise également un algorithme de recherche en profondeur pour renseigner les résultats obtenus avec des détails sur l'emplacement des occurrences spécifiques de données sensibles que Macie trouve dans les objets S3. Ces occurrences fournissent des informations sur les catégories et les types de données

sensibles qu'un compartiment et un objet S3 peuvent contenir. Les détails peuvent vous aider à localiser les occurrences individuelles de données sensibles dans des objets et à déterminer s'il convient d'effectuer une analyse plus approfondie de compartiments et d'objets spécifiques.

Grâce aux données sensibles trouvées, vous pouvez déterminer l'emplacement de 15 occurrences de données sensibles détectées par Macie dans un objet S3 affecté. Cela inclut les données sensibles que Macie a détectées à l'aide d'identifiants de données gérés et les données qui correspondent aux critères des identifiants de données personnalisés que vous avez configuré pour une tâche ou que Macie doit utiliser.

Une recherche de données sensibles peut fournir des détails tels que :

- Numéro de colonne et de ligne d'une cellule ou d'un champ dans un classeur Microsoft Excel, un fichier CSV ou un fichier TSV.
- Le chemin d'accès à un champ ou à un tableau dans un fichier JSON ou JSON Lines.
- Le numéro de ligne d'une ligne d'un fichier texte non binaire autre qu'un fichier CSV, JSON, JSON Lines ou TSV (par exemple, un fichier HTML, TXT ou XML).
- Numéro de page d'une page dans un fichier Adobe Portable Document Format (PDF).
- L'index de l'enregistrement et le chemin d'accès à un champ d'un enregistrement d'un conteneur d'objets Apache Avro ou d'un fichier Apache Parquet.

Vous pouvez accéder à ces informations à l'aide de la console Amazon Macie ou de l'API Amazon Macie ou Macie ie ie Macie ou Amazon Macie ie ie ie API. Vous pouvez également accéder à ces informations dans les résultats que Macie publie sur d'autres sitesServices AWS, à la fois Amazon EventBridge etAWS Security Hub. Pour en savoir plus sur les structures JSON que Macie utilise pour rapporter ces détails, consultezSchéma JSON pour les emplacements de données sensibles. Pour savoir comment accéder aux détails des résultats que Macie publie à d'autresServices AWS, voirSurveillance et traitement des résultats.

Si un objet S3 contient de nombreuses occurrences de données sensibles, vous pouvez également utiliser une recherche pour accéder au résultat de découverte de données sensibles correspondant. Contrairement à la recherche de données sensibles, un résultat de découverte de données sensibles fournit des données de localisation détaillées pour jusqu'à 1 000 occurrences de chaque type de données sensibles que Macie a trouvé dans un objet. Si un objet S3 est un fichier d'archive, tel qu'un fichier .tar ou .zip, cela inclut les occurrences de données sensibles dans des fichiers individuels que Macie a extraits de l'archive. (Macie n'inclut pas ces informations dans les résultats relatifs aux données sensibles.) Pour en savoir plus sur les résultats de la découverte de données sensibles,

consultezStockage et conservation des résultats de découverte de données sensibles. Macie utilise le même schéma pour les données de localisation dans les résultats de recherche de données sensibles et dans les résultats de découverte de données sensibles.

Localisation des occurrences de données sensibles

Pour localiser les occurrences de données sensibles, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie. Les étapes suivantes vous expliquent comment localiser les données sensibles à l'aide de la console.

Pour localiser des données sensibles par programmation, utilisez le GetFindingsfonctionnement de l'API Amazon Macie. Si une constatation inclut des détails concernant l'emplacement d'une ou de plusieurs occurrences d'un type spécifique de données sensibles, `occurrences` les objets de la constatation fournissent ces informations. Pour plus d'informations, veuillez consulter Schéma JSON pour les emplacements de données sensibles.

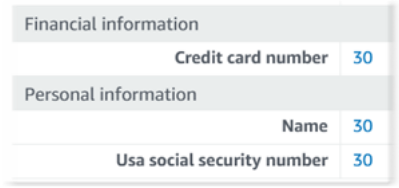
Pour localiser les occurrences de données sensibles

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Conclusions.

   > **Tip**
   >
   > Vous pouvez utiliser la page Tâches pour afficher tous les résultats d'une tâche de découverte de données sensibles particulière. Pour ce faire, sélectionnez Jobs dans le panneau de navigation, puis sélectionnez le nom du job. En haut du panneau de détails, choisissez Afficher les résultats, puis Afficher les résultats.

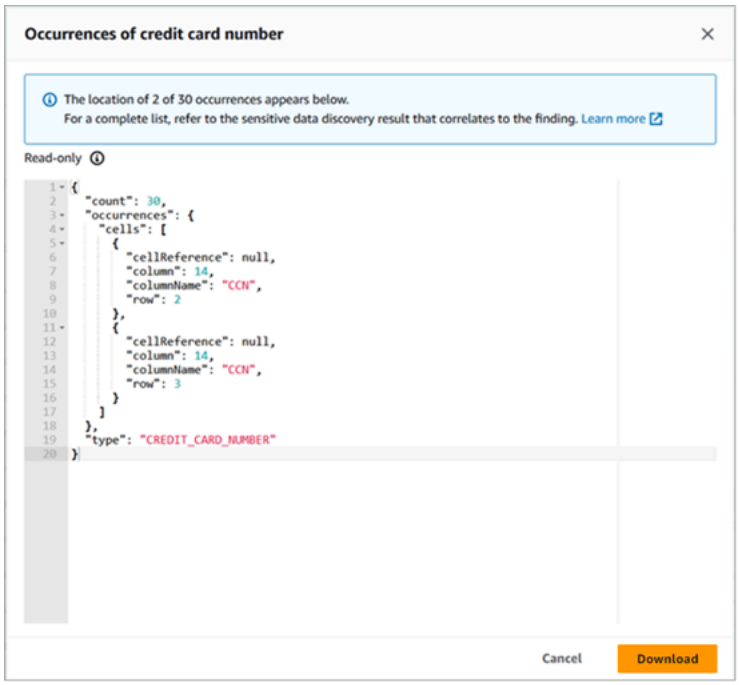
3. Sur la page Find occurrences occurrences occurrences occurrences des résultats sensibles que vous souhaitez localiser, sélectionnez la recherche des données sensibles que vous souhaitez localiser. Le panneau des détails affiche des informations relatives au résultat.
4. Dans le panneau des détails, accédez à la section Données sensibles. Cette section fournit des informations sur les catégories et les types de données sensibles que Macie a trouvées dans l'objet S3 concerné. Il indique également le nombre d'occurrences de chaque type de données sensibles détectées par Macie.

   Par exemple, l'image suivante montre certains détails d'une constatation faisant état de 30 occurrences de numéros de carte de crédit, 30 occurrences de noms et 30 occurrences de numéros de sécurité sociale américains.



Si la recherche inclut des détails concernant l'emplacement d'une ou de plusieurs occurrences d'un type spécifique de données sensibles, le nombre d'occurrences est un lien. Cliquez sur le lien pour afficher les détails. Macie ouvre une nouvelle fenêtre et affiche les détails au format JSON.

Par exemple, l'image suivante montre l'emplacement de deux occurrences de numéros de carte de crédit dans un objet S3 concerné.



Pour enregistrer les détails sous forme de fichier JSON, choisissez Télécharger, puis spécifiez un nom et un emplacement pour le fichier.

5. (Facultatif) Pour enregistrer tous les détails de la recherche dans un fichier JSON, choisissez l'identifiant de la recherche (Finding ID) en haut du panneau des détails. Macie ouvre une nouvelle fenêtre et affiche tous les détails au format JSON. Choisissez Télécharger, puis spécifiez un nom et un emplacement pour le fichier.

Pour accéder aux détails concernant l'emplacement de pas moins de 1 000 occurrences de chaque type de données sensibles dans l'objet concerné, reportez-vous au résultat de découverte de

données sensibles correspondant à la découverte. Pour ce faire, accédez au début de la section Détails du panneau. Cliquez ensuite sur le lien dans le champ Emplacement détaillé des résultats. Macie ouvre la console Amazon S3 et affiche le fichier ou le dossier contenant le résultat de découverte correspondant.

Extraction d'échantillons de données sensibles grâce aux résultats d'Amazon Macie

Pour vérifier la nature des données sensibles signalées par Amazon Macie dans les résultats, vous pouvez éventuellement configurer et utiliser Macie pour récupérer et révéler des échantillons de données sensibles signalées par des résultats individuels. Cela inclut les données sensibles détectées par Macie à l'aide d'identifiants de données gérés et les données qui répondent aux critères des identifiants de données personnalisés. Les exemples peuvent vous aider à personnaliser votre enquête sur un objet ou un bucket Amazon Simple Storage Service (Amazon S3) concernés.

Si vous récupérez et révélez des échantillons de données sensibles pour une recherche, Macie exécute les tâches générales suivantes :

1. Vérifie que le résultat indique l'emplacement des occurrences individuelles de données sensibles et l'emplacement du résultat de découverte de données sensibles correspondant.
2. Évalue le résultat de découverte de données sensibles correspondant, en vérifiant la validité des métadonnées de l'objet S3 concerné et des données de localisation pour détecter les occurrences de données sensibles dans l'objet.
3. En utilisant les données dans le résultat de la découverte de données sensibles, localise les 1 à 10 premières occurrences de données sensibles signalées par la découverte et extrait les 1 à 128 premiers caractères de chaque occurrence de l'objet S3 concerné. Si la découverte fait état de plusieurs types de données sensibles, Macie le fait pour un maximum de 100 types.
4. Chiffre les données extraites avec une clé AWS Key Management Service (AWS KMS) que vous spécifiez.
5. Stocke temporairement les données chiffrées dans un cache et les affiche pour que vous puissiez les consulter. Les données sont cryptées à tout moment, à la fois en transit et au repos.
6. Peu après l'extraction et le chiffrement, supprime définitivement les données du cache, sauf si une conservation supplémentaire est temporairement requise pour résoudre un problème opérationnel.

Si vous choisissez de récupérer et de révéler des échantillons de données sensibles pour une nouvelle recherche, Macie répète ces tâches pour localiser, extraire, chiffrer, stocker et finalement supprimer les échantillons.

Macie n'utilise pas le rôle lié au service Macie pour votre compte pour effectuer ces tâches. Au lieu de cela, vous utilisez votre identité AWS Identity and Access Management (IAM) ou vous autorisez Macie à assumer un rôle IAM dans votre compte. Vous pouvez récupérer et révéler des échantillons de données sensibles à des fins de recherche si vous ou le rôle êtes autorisé à accéder aux ressources et aux données requises et à effectuer les actions requises. Toutes les actions requises sont enregistrées. AWS CloudTrail

> **Important**
>
> Nous vous recommandons de restreindre l'accès à cette fonctionnalité en utilisant des politiques IAM personnalisées. Pour un contrôle d'accès supplémentaire, nous vous recommandons également de créer un système dédié au AWS KMS key chiffrement des échantillons de données sensibles récupérés, et de limiter l'utilisation de la clé aux personnes principales qui doivent être autorisées à récupérer et à révéler des échantillons de données sensibles.
>
> Pour obtenir des recommandations et des exemples de politiques que vous pouvez utiliser pour contrôler l'accès à cette fonctionnalité, consultez le billet de blog Comment utiliser Amazon Macie pour prévisualiser des données sensibles dans des compartiments S3 sur le AWS blog de sécurité.

Les rubriques de cette section expliquent comment configurer et utiliser Macie pour récupérer et révéler des échantillons de données sensibles à des fins de recherche. Vous pouvez effectuer ces tâches dans tous les Régions AWS endroits où Macie est actuellement disponible, à l'exception des régions Asie-Pacifique (Osaka) et Israël (Tel Aviv).

Rubriques

- Options de configuration et exigences pour récupérer des échantillons de données sensibles contenant des résultats
- Configuration d'Amazon Macie pour récupérer et révéler des échantillons de données sensibles contenant des résultats
- Extraction et divulgation d'échantillons de données sensibles accompagnés de résultats

Options de configuration et exigences pour récupérer des échantillons de données sensibles contenant des résultats

Vous pouvez éventuellement configurer et utiliser Amazon Macie pour récupérer et révéler des échantillons de données sensibles que Macie rapporte dans des résultats individuels. Si vous récupérez et révélez des échantillons de données sensibles à des fins de recherche, Macie utilise les données du résultat de découverte de données sensibles correspondant pour localiser les occurrences de données sensibles dans l'objet Amazon Simple Storage Service (Amazon S3) concerné. Macie extrait ensuite des échantillons de ces occurrences de l'objet concerné. Macie chiffre les données extraites avec une clé AWS Key Management Service (AWS KMS) que vous spécifiez, stocke temporairement les données chiffrées dans un cache et renvoie les données dans vos résultats pour la recherche. Peu après l'extraction et le chiffrement, Macie supprime définitivement les données du cache, sauf si une conservation supplémentaire est temporairement requise pour résoudre un problème de fonctionnement.

Macie n'utilise pas le rôle lié au service Macie pour votre compte pour localiser, récupérer, chiffrer ou révéler des échantillons de données sensibles pour les objets S3 concernés. Macie utilise plutôt les paramètres et les ressources que vous configurez pour votre compte. Lorsque vous configurez les paramètres dans Macie, vous spécifiez comment accéder aux objets S3 concernés. Vous spécifiez également celui AWS KMS key à utiliser pour chiffrer les échantillons. Vous pouvez configurer les paramètres dans toutes les régions Régions AWS où Macie est actuellement disponible, à l'exception des régions Asie-Pacifique (Osaka) et Israël (Tel Aviv).

Pour accéder aux objets S3 concernés et en extraire des échantillons de données sensibles, deux options s'offrent à vous. Vous pouvez configurer Macie pour qu'il utilise les informations d'identification utilisateur AWS Identity and Access Management (IAM) ou qu'il assume un rôle IAM :

- Utiliser les informations d'identification de l'utilisateur IAM : avec cette option, chaque utilisateur de votre compte utilise son identité IAM individuelle pour localiser, récupérer, chiffrer et révéler les échantillons. Cela signifie qu'un utilisateur peut récupérer et révéler des échantillons de données sensibles à des fins de recherche s'il est autorisé à accéder aux ressources et aux données requises et à effectuer les actions requises.
- Assumez un rôle IAM : avec cette option, vous créez un rôle IAM qui délègue l'accès à Macie. Vous vous assurez également que les politiques de confiance et d'autorisation relatives au rôle répondent à toutes les exigences pour que Macie assume le rôle. Macie assume ensuite le rôle lorsqu'un utilisateur de votre compte choisit de localiser, de récupérer, de chiffrer et de révéler des échantillons de données sensibles à des fins de recherche.

Vous pouvez utiliser l'une ou l'autre configuration avec n'importe quel type de compte Macie : un compte administrateur Macie délégué pour une organisation, un compte de membre Macie dans une organisation ou un compte Macie autonome.

Les rubriques suivantes décrivent les options, les exigences et les considérations qui peuvent vous aider à déterminer comment configurer les paramètres et les ressources de votre compte. Cela inclut les politiques de confiance et d'autorisation à associer à un rôle IAM. Pour obtenir des recommandations supplémentaires et des exemples de politiques que vous pouvez utiliser pour récupérer et révéler des échantillons de données sensibles, consultez le billet de blog Comment utiliser Amazon Macie pour prévisualiser les données sensibles dans des compartiments S3 sur le AWS blog de sécurité.

Rubriques

Déterminer la méthode d'accès à utiliser

Lorsque vous déterminez quelle configuration convient le mieux à votre AWS environnement, il est essentiel de déterminer si celui-ci inclut plusieurs comptes Amazon Macie gérés de manière centralisée en tant qu'organisation. Si vous êtes l'administrateur Macie délégué d'une organisation, configurer Macie pour qu'il assume un rôle IAM peut rationaliser la récupération d'échantillons de données sensibles à partir des objets S3 concernés pour les comptes de votre organisation. Cette approche vous permet de créer un rôle IAM dans votre compte administrateur. Vous créez également un rôle IAM dans chaque compte membre applicable. Le rôle de votre compte administrateur délègue l'accès à Macie. Le rôle d'un compte membre délègue l'accès entre comptes au rôle de votre compte administrateur. S'il est implémenté, vous pouvez ensuite utiliser le chaînage des rôles pour accéder aux objets S3 concernés pour vos comptes membres.

Déterminez également qui a un accès direct aux résultats individuels par défaut. Pour récupérer et révéler des échantillons de données sensibles pour une découverte, un utilisateur doit d'abord avoir accès à la constatation :

- Tâches de découverte de données sensibles : seul le compte qui crée une tâche peut accéder aux résultats produits par cette tâche. Si vous avez un compte administrateur Macie, vous pouvez configurer une tâche pour analyser des objets dans des compartiments S3 pour n'importe quel compte de votre organisation. Par conséquent, vos tâches peuvent générer des résultats pour des objets se trouvant dans des compartiments appartenant à vos comptes membres. Si vous avez un compte membre ou un compte Macie autonome, vous pouvez configurer une tâche pour analyser les objets uniquement dans les buckets détenus par votre compte.
- Découverte automatique des données sensibles : seul le compte administrateur Macie peut accéder aux résultats produits par la découverte automatique pour les comptes de son organisation. Les comptes des membres ne peuvent pas accéder à ces résultats. Si vous possédez un compte Macie autonome, vous pouvez accéder aux résultats que la découverte automatique produit uniquement pour votre propre compte.

Si vous prévoyez d'accéder aux objets S3 concernés à l'aide d'un rôle IAM, tenez également compte des points suivants :

- Pour localiser les occurrences de données sensibles dans un objet, le résultat de découverte de données sensibles correspondant à une recherche doit être stocké dans un objet S3 que Macie a signé avec un code d'authentification de message basé sur le hachage (HMAC). AWS KMS key Macie doit être en mesure de vérifier l'intégrité et l'authenticité du résultat de la découverte de données sensibles. Sinon, Macie n'assume pas le rôle IAM pour récupérer des échantillons de données sensibles. Il s'agit d'un garde-fou supplémentaire permettant de restreindre l'accès aux données d'un compte dans les objets S3.
- Pour récupérer des échantillons de données sensibles à partir d'un objet chiffré géré par un clientAWS KMS key, le rôle IAM doit être autorisé à déchiffrer les données à l'aide de la clé. Plus précisément, la politique de la clé doit permettre au rôle d'exécuter l'`kms:Decrypt`action. Pour les autres types de chiffrement côté serveur, aucune autorisation ou ressource supplémentaire n'est requise pour déchiffrer un objet concerné. Pour plus d'informations, consultez Décryptage des objets S3 concernés.
- Pour récupérer des échantillons de données sensibles d'un objet pour un autre compte, vous devez actuellement être l'administrateur Macie délégué du compte dans le compte applicableRégion AWS. En outre :
  - Macie doit actuellement être activé pour le compte membre dans la région applicable.

- Le compte membre doit avoir un rôle IAM qui délègue l'accès entre comptes à un rôle IAM dans votre compte administrateur Macie. Le nom du rôle doit être le même dans votre compte administrateur Macie et dans le compte membre.
- La politique de confiance pour le rôle IAM dans le compte membre doit inclure une condition qui spécifie l'ID externe correct pour votre configuration. Cet identifiant est une chaîne alphanumérique unique que Macie génère automatiquement une fois que vous avez configuré les paramètres de votre compte administrateur Macie. Pour plus d'informations sur l'utilisation d'identifiants externes dans les politiques de confiance, voir Comment utiliser un identifiant externe lorsque vous accordez l'accès à vos AWS ressources à un tiers dans le Guide de AWS Identity and Access Management l'utilisateur.
- Si le rôle IAM dans le compte membre répond à toutes les exigences de Macie, le compte membre n'a pas besoin de configurer et d'activer les paramètres Macie pour que vous puissiez récupérer des échantillons de données sensibles à partir d'objets pour son compte. Macie utilise uniquement les paramètres et le rôle IAM dans votre compte administrateur Macie et le rôle IAM dans le compte membre.

> **Tip**
>
> Si votre compte fait partie d'une grande organisation, pensez à utiliser un AWS CloudFormation modèle et un ensemble de piles pour attribuer et gérer les rôles IAM pour les comptes des membres de votre organisation. Pour plus d'informations sur la création et l'utilisation de modèles et de jeux de piles, consultez le guide de AWS CloudFormation l'utilisateur.
>
> Pour consulter et éventuellement télécharger un CloudFormation modèle pouvant servir de point de départ, vous pouvez utiliser la console Amazon Macie. Dans le volet de navigation de la console, sous Paramètres, sélectionnez Afficher les échantillons. Choisissez Modifier, puis Afficher les autorisations et le CloudFormation modèle des rôles des membres.

Les rubriques suivantes de cette section fournissent des informations et des considérations supplémentaires pour chaque type de configuration. Pour les rôles IAM, cela inclut les politiques de confiance et d'autorisation à associer à un rôle. Si vous ne savez pas quel type de configuration convient le mieux à votre environnement, demandez de l'aide à votre AWS administrateur.

Utilisation des informations d'identification utilisateur IAM pour accéder aux objets S3 concernés

Si vous configurez Amazon Macie pour récupérer des échantillons de données sensibles à l'aide des informations d'identification utilisateur IAM, chaque utilisateur de votre compte Macie utilise son identité IAM pour localiser, récupérer, chiffrer et révéler des échantillons pour des résultats individuels. Cela signifie qu'un utilisateur peut récupérer et révéler des échantillons de données sensibles afin de déterminer si son identité IAM est autorisée à accéder aux ressources et aux données requises et à effectuer les actions requises. Toutes les actions requises sont enregistrées. AWS CloudTrail

Pour récupérer et révéler des échantillons de données sensibles pour une découverte particulière, un utilisateur doit être autorisé à accéder aux données et ressources suivantes : la recherche, le résultat de découverte de données sensibles correspondant, le compartiment S3 concerné et l'objet S3 concerné. Ils doivent également être autorisés à utiliser celui AWS KMS key qui a été utilisé pour chiffrer l'objet concerné, le cas échéant, et AWS KMS key celui que vous avez configuré Macie pour chiffrer des échantillons de données sensibles. Si des politiques IAM, des politiques de ressources ou d'autres paramètres d'autorisation refusent l'accès requis, l'utilisateur ne sera pas en mesure de récupérer et de révéler des échantillons pour la recherche.

Pour configurer ce type de configuration, effectuez les tâches générales suivantes :

1. Vérifiez que vous avez configuré un référentiel pour les résultats de la découverte de vos données sensibles.
2. Configurez le AWS KMS key à utiliser pour le chiffrement d'échantillons de données sensibles.
3. Vérifiez vos autorisations pour configurer les paramètres dans Macie.
4. Configurez et activez les paramètres dans Macie.

Pour plus d'informations sur l'exécution de ces tâches, consultezConfiguration d'Amazon Macie pour récupérer et révéler des échantillons de données sensibles contenant des résultats.

Assumer un rôle IAM pour accéder aux objets S3 concernés

Pour configurer Amazon Macie afin de récupérer des échantillons de données sensibles en assumant un rôle IAM, commencez par créer un rôle IAM qui délègue l'accès à Macie. Assurez-vous que les politiques de confiance et d'autorisation relatives au rôle répondent à toutes les exigences pour que Macie assume le rôle. Lorsqu'un utilisateur de votre compte Macie choisit ensuite de récupérer et de révéler des échantillons de données sensibles à des fins de recherche, Macie assume le rôle

de récupérer les échantillons de l'objet S3 concerné. Macie assume le rôle uniquement lorsqu'un utilisateur choisit de récupérer et de révéler des échantillons à des fins de recherche. Pour assumer ce rôle, Macie utilise le AssumeRolefonctionnement de l'API AWS Security Token Service (AWS STS). Toutes les actions requises sont enregistrées. AWS CloudTrail

Pour récupérer et révéler des échantillons de données sensibles pour une découverte particulière, un utilisateur doit être autorisé à accéder à la découverte de données sensibles, au résultat de découverte de données sensibles correspondant et au AWS KMS key fichier que vous configurez Macie pour chiffrer les échantillons de données sensibles. Le rôle IAM doit permettre à Macie d'accéder au compartiment S3 et à l'objet S3 concernés. Le rôle doit également être autorisé à utiliser celui AWS KMS key qui a été utilisé pour chiffrer l'objet concerné, le cas échéant. Si des politiques IAM, des politiques de ressources ou d'autres paramètres d'autorisation refusent l'accès requis, l'utilisateur ne sera pas en mesure de récupérer et de révéler des échantillons pour la recherche.

Pour configurer ce type de configuration, effectuez les tâches générales suivantes. Si vous avez un compte membre dans une organisation, contactez votre administrateur Macie pour déterminer si et comment configurer les paramètres et les ressources de votre compte.

1. Définissez les éléments suivants :
   - Nom du rôle IAM que vous souhaitez que Macie assume. Si votre compte fait partie d'une organisation, ce nom doit être le même pour le compte administrateur Macie délégué et pour chaque compte de membre applicable de l'organisation. Dans le cas contraire, l'administrateur Macie ne pourra pas accéder aux objets S3 concernés pour un compte de membre applicable.
   - Nom de la politique d'autorisations IAM à associer au rôle IAM. Si votre compte fait partie d'une organisation, nous vous recommandons d'utiliser le même nom de politique pour chaque compte membre applicable de l'organisation. Cela permet de rationaliser le provisionnement et la gestion du rôle dans les comptes des membres.
2. Vérifiez que vous avez configuré un référentiel pour les résultats de la découverte de vos données sensibles.
3. Configurez le AWS KMS key à utiliser pour le chiffrement d'échantillons de données sensibles.
4. Vérifiez vos autorisations pour créer des rôles IAM et configurer les paramètres dans Macie.
5. Si vous êtes l'administrateur Macie délégué d'une organisation ou si vous possédez un compte Macie autonome :
   a. Créez et configurez le rôle IAM pour votre compte. Assurez-vous que les politiques de confiance et d'autorisation relatives au rôle répondent à toutes les exigences pour que Macie assume le rôle. Pour plus de détails sur ces exigences, consultez la rubrique suivante.

b. Configurez et activez les paramètres dans Macie. Macie génère ensuite un identifiant externe pour la configuration. Si vous êtes l'administrateur Macie d'une organisation, notez cet identifiant. La politique de confiance pour le rôle IAM dans chacun de vos comptes membres applicables doit spécifier cet ID.

6. Si vous avez un compte membre dans une organisation :

   a. Demandez à votre administrateur Macie l'ID externe à spécifier dans la politique de confiance pour le rôle IAM dans votre compte. Vérifiez également le nom du rôle IAM et la politique d'autorisations à créer.

   b. Créez et configurez le rôle IAM pour votre compte. Assurez-vous que les politiques de confiance et d'autorisation relatives au rôle répondent à toutes les exigences pour que votre administrateur Macie assume le rôle. Pour plus de détails sur ces exigences, consultez la rubrique suivante.

   c. (Facultatif) Si vous souhaitez récupérer et révéler des échantillons de données sensibles provenant des objets S3 concernés pour votre propre compte, configurez et activez les paramètres dans Macie. Si vous souhaitez que Macie assume un rôle IAM pour récupérer les échantillons, commencez par créer et configurer un rôle IAM supplémentaire dans votre compte. Assurez-vous que les politiques de confiance et d'autorisation pour ce rôle supplémentaire répondent à toutes les exigences pour que Macie assume le rôle. Configurez ensuite les paramètres dans Macie et spécifiez le nom de ce rôle supplémentaire. Pour plus de détails sur les exigences de politique relatives au rôle, consultez la rubrique suivante.

Pour plus d'informations sur l'exécution de ces tâches, consultezConfiguration d'Amazon Macie pour récupérer et révéler des échantillons de données sensibles contenant des résultats.

Configuration d'un rôle IAM pour accéder aux objets S3 concernés

Pour accéder aux objets S3 concernés à l'aide d'un rôle IAM, commencez par créer et configurer un rôle qui délègue l'accès à Amazon Macie. Assurez-vous que les politiques de confiance et d'autorisation relatives au rôle répondent à toutes les exigences pour que Macie assume le rôle. La façon de procéder dépend du type de compte Macie que vous possédez.

Les sections suivantes fournissent des détails sur les politiques de confiance et d'autorisation à associer au rôle IAM pour chaque type de compte Macie. Choisissez la section correspondant au type de compte que vous possédez.

> **Note**
>
> Si vous avez un compte membre dans une organisation, vous devrez peut-être créer et configurer deux rôles IAM pour votre compte :
>
> - Pour permettre à votre administrateur Macie de récupérer et de révéler des échantillons de données sensibles provenant des objets S3 concernés pour votre compte, créez et configurez un rôle que le compte de votre administrateur peut assumer. Pour plus de détails, choisissez la section du compte de membre Macie.
> - Pour récupérer et révéler des échantillons de données sensibles provenant des objets S3 concernés pour votre propre compte, créez et configurez un rôle que Macie peut assumer. Pour plus de détails, choisissez la section Compte Macie autonome.
>
> Avant de créer et de configurer l'un des rôles IAM, contactez votre administrateur Macie pour déterminer la configuration appropriée pour votre compte.

Pour obtenir des informations détaillées sur l'utilisation d'IAM pour créer le rôle, consultez la section Création d'un rôle à l'aide de politiques de confiance personnalisées dans le Guide de AWS Identity and Access Management l'utilisateur.

Compte administrateur Macie

Si vous êtes l'administrateur Macie délégué d'une organisation, commencez par utiliser l'éditeur de stratégie IAM pour créer la politique d'autorisations pour le rôle IAM. La politique doit être la suivante.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        },
        {
```

```
            "Sid": "AssumeMacieRevealRoleForCrossAccountAccess",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "arn:aws:iam::*:role/IAMRoleName"
        }
    ]
}
```

Où *IAM RoleName* est le nom du rôle IAM que Macie doit assumer lors de la récupération d'échantillons de données sensibles à partir d'objets S3 concernés pour les comptes de votre organisation. Remplacez cette valeur par le nom du rôle que vous créez pour votre compte et que vous prévoyez de créer pour les comptes membres applicables de votre organisation. Ce nom doit être le même pour votre compte administrateur Macie et pour chaque compte de membre applicable.

> **Note**
>
> Dans la politique d'autorisation précédente, l'`Resource`élément de la première instruction utilise un caractère générique (*). Cela permet à une entité IAM attachée de récupérer des objets dans tous les compartiments S3 que possède votre organisation. Pour autoriser cet accès uniquement à des compartiments spécifiques, remplacez le caractère générique par le nom de ressource Amazon (ARN) de chaque compartiment. Par exemple, pour autoriser l'accès uniquement aux objets d'un compartiment nommé DOC-EXAMPLE-BUCKET, modifiez l'élément comme suit :
> `"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"`
> Vous pouvez également restreindre l'accès aux objets dans des compartiments S3 spécifiques pour des comptes individuels. Pour ce faire, spécifiez les ARN du bucket dans l'`Resource`élément de la politique d'autorisation pour le rôle IAM dans chaque compte applicable. Pour plus d'informations et des exemples, voir Éléments de politique IAM JSON : ressource dans le guide de l'AWS Identity and Access Managementutilisateur.

Après avoir créé la politique d'autorisations pour le rôle IAM, créez et configurez le rôle. Si vous le faites à l'aide de la console IAM, choisissez Custom trust policy comme type d'entité fiable pour le rôle. Pour la politique de confiance qui définit les entités fiables pour le rôle, spécifiez ce qui suit.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AllowMacieReveal",
            "Effect": "Allow",
            "Principal": {
                "Service": "reveal-samples.macie.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "accountID"
                }
            }
        }
    ]
}
```

Où *AccountID* est l'identifiant de compte de votre. Compte AWS Remplacez cette valeur par votre identifiant de compte à 12 chiffres.

Dans la politique de confiance précédente :

- L'`Principal`élément spécifie le principal de service que Macie utilise lors de la récupération d'échantillons de données sensibles à partir d'objets S3 concernés. `reveal-samples.macie.amazonaws.com`
- L'`Action`élément spécifie l'action que le principal de service est autorisé à effectuer, le AssumeRolefonctionnement de l'API AWS Security Token Service (AWS STS).
- L'`Condition`élément définit une condition qui utilise la clé de contexte aws : SourceAccount global condition. Cette condition détermine quel compte peut effectuer l'action spécifiée. Dans ce cas, cela permet à Macie d'assumer le rôle uniquement pour le compte spécifié (*AccountID*). Cette condition permet d'éviter que Macie ne soit utilisée comme une adjointe confuse lors de transactions avecAWS STS.

Après avoir défini la politique de confiance pour le rôle IAM, associez la politique d'autorisations au rôle. Il doit s'agir de la politique d'autorisation que vous avez créée avant de commencer à créer le rôle. Effectuez ensuite les étapes restantes dans IAM pour terminer la création et la configuration du rôle. Lorsque vous avez terminé, configurez et activez les paramètres dans Macie.

Compte membre Macie

Si vous avez un compte de membre Macie et que vous souhaitez autoriser votre administrateur Macie à récupérer et à révéler des échantillons de données sensibles provenant des objets S3 concernés pour votre compte, commencez par demander les informations suivantes à votre administrateur Macie :

- Nom du rôle IAM à créer. Le nom de votre compte doit être le même que celui du compte administrateur Macie de votre organisation.
- Nom de la politique d'autorisations IAM à associer au rôle.
- ID externe à spécifier dans la politique de confiance du rôle. Cet identifiant doit être l'identifiant externe généré par Macie pour la configuration de votre administrateur Macie.

Après avoir reçu ces informations, utilisez l'éditeur de stratégie IAM pour créer la politique d'autorisations pour le rôle. La politique doit être la suivante.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

La politique d'autorisation précédente permet à une entité IAM attachée de récupérer des objets de tous les compartiments S3 de votre compte. Cela est dû au fait que l'`Resource`élément de la politique utilise un caractère générique (*). Pour autoriser cet accès uniquement à des compartiments spécifiques, remplacez le caractère générique par le nom de ressource Amazon (ARN) de chaque compartiment. Par exemple, pour autoriser l'accès uniquement aux objets d'un compartiment nommé DOC-EXAMPLE-BUCKET2, modifiez l'élément comme suit :

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2/*"
```

Pour plus d'informations et des exemples, voir Éléments de politique IAM JSON : ressource dans le guide de l'AWS Identity and Access Managementutilisateur.

Après avoir créé la politique d'autorisations pour le rôle IAM, créez le rôle. Si vous créez le rôle à l'aide de la console IAM, choisissez Custom trust policy comme type d'entité fiable pour le rôle. Pour la politique de confiance qui définit les entités fiables pour le rôle, spécifiez ce qui suit.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieAdminRevealRoleForCrossAccountAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::administratorAccountID:role/IAMRoleName"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "sts:ExternalId": "externalID",
                    "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
                }
            }
        }
    ]
}
```

Dans la politique précédente, remplacez les valeurs d'espace réservé par les valeurs correctes pour votre AWS environnement, où :

- *AdministratorAccountId* est l'identifiant de compte à 12 chiffres du compte de votre administrateur Macie.
- *IAM RoleName* est le nom du rôle IAM dans le compte de votre administrateur Macie. Il doit s'agir du nom que vous avez reçu de votre administrateur Macie.
- *ExternalID* est l'ID externe que vous avez reçu de votre administrateur Macie.

En général, la politique de confiance permet à votre administrateur Macie d'assumer le rôle de récupérer et de révéler des échantillons de données sensibles provenant des objets S3 concernés pour votre compte. L'`Principal`élément spécifie l'ARN d'un rôle IAM dans le compte de votre administrateur Macie. C'est le rôle que votre administrateur Macie utilise pour récupérer et révéler

des échantillons de données sensibles pour les comptes de votre organisation. Le `Condition` bloc définit deux conditions qui déterminent en outre qui peut assumer le rôle :

- La première condition spécifie un identifiant externe propre à la configuration de votre organisation. Pour en savoir plus sur les identifiants externes, consultez la section Comment utiliser un identifiant externe lorsque vous accordez l'accès à vos AWS ressources à un tiers dans le Guide de AWS Identity and Access Management l'utilisateur.
- La deuxième condition utilise la clé de contexte de condition globale aws : PrincipalOrg ID. La valeur de la clé est une variable dynamique qui représente l'identifiant unique d'une organisation dans AWS Organizations (`${aws:ResourceOrgID}`). La condition restreint l'accès aux seuls comptes appartenant à la même organisation dansAWS Organizations. Si vous avez rejoint votre organisation en acceptant une invitation dans Macie, supprimez cette condition de la politique.

Après avoir défini la politique de confiance pour le rôle IAM, associez la politique d'autorisations au rôle. Il doit s'agir de la politique d'autorisation que vous avez créée avant de commencer à créer le rôle. Effectuez ensuite les étapes restantes dans IAM pour terminer la création et la configuration du rôle. Ne configurez pas et ne saisissez pas les paramètres du rôle dans Macie.

Compte Macie autonome

Si vous avez un compte Macie autonome ou un compte membre Macie et que vous souhaitez récupérer et révéler des échantillons de données sensibles provenant d'objets S3 concernés pour votre propre compte, commencez par utiliser l'éditeur de stratégie IAM pour créer la politique d'autorisations pour le rôle IAM. La politique doit être la suivante.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RetrieveS3Objects",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
```

```
}
```

Dans la politique d'autorisation précédente, l'`Resource`élément utilise un caractère générique (*). Cela permet à une entité IAM attachée de récupérer des objets dans tous les compartiments S3 de votre compte. Pour autoriser cet accès uniquement à des compartiments spécifiques, remplacez le caractère générique par le nom de ressource Amazon (ARN) de chaque compartiment. Par exemple, pour autoriser l'accès uniquement aux objets d'un compartiment nommé DOC-EXAMPLE-BUCKET3, modifiez l'élément comme suit :

```
"Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET3/*"
```

Pour plus d'informations et des exemples, voir Éléments de politique IAM JSON : ressource dans le guide de l'AWS Identity and Access Managementutilisateur.

Après avoir créé la politique d'autorisations pour le rôle IAM, créez le rôle. Si vous créez le rôle à l'aide de la console IAM, choisissez Custom trust policy comme type d'entité fiable pour le rôle. Pour la politique de confiance qui définit les entités fiables pour le rôle, spécifiez ce qui suit.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowMacieReveal",
            "Effect": "Allow",
            "Principal": {
                "Service": "reveal-samples.macie.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "accountID"
                }
            }
        }
    ]
}
```

Où *`AccountID`* est l'identifiant de compte de votre. Compte AWS Remplacez cette valeur par votre identifiant de compte à 12 chiffres.

Dans la politique de confiance précédente :

- L'`Principal`élément spécifie le principal de service que Macie utilise pour récupérer et révéler des échantillons de données sensibles provenant d'objets S3 concernés. `reveal-samples.macie.amazonaws.com`
- L'`Action`élément spécifie l'action que le principal de service est autorisé à effectuer, le AssumeRolefonctionnement de l'API AWS Security Token Service (AWS STS).
- L'`Condition`élément définit une condition qui utilise la clé de contexte aws : SourceAccount global condition. Cette condition détermine quel compte peut effectuer l'action spécifiée. Cela permet à Macie d'assumer le rôle uniquement pour le compte spécifié (*`AccountID`*). Cette condition permet d'éviter que Macie ne soit utilisée comme une adjointe confuse lors de transactions avecAWS STS.

Après avoir défini la politique de confiance pour le rôle IAM, associez la politique d'autorisations au rôle. Il doit s'agir de la politique d'autorisation que vous avez créée avant de commencer à créer le rôle. Effectuez ensuite les étapes restantes dans IAM pour terminer la création et la configuration du rôle. Lorsque vous avez terminé, configurez et activez les paramètres dans Macie.

Décryptage des objets S3 concernés

Amazon S3 prend en charge plusieurs options de chiffrement pour les objets S3. Pour la plupart de ces options, aucune ressource ou autorisation supplémentaire n'est requise pour qu'un utilisateur ou un rôle IAM puisse déchiffrer et récupérer des échantillons de données sensibles d'un objet concerné. C'est le cas d'un objet chiffré à l'aide d'un chiffrement côté serveur à l'aide d'une clé gérée par Amazon S3 ou d'une AWS clé gérée. AWS KMS key

Toutefois, si un objet S3 est chiffré et géré par un clientAWS KMS key, des autorisations supplémentaires sont nécessaires pour déchiffrer et récupérer des échantillons de données sensibles de l'objet. Plus précisément, la politique de clé pour la clé KMS doit autoriser l'utilisateur ou le rôle IAM à effectuer l'`kms:Decrypt`action. Sinon, une erreur se produit et Macie ne récupère aucun échantillon de l'objet. Pour savoir comment fournir cet accès à un utilisateur IAM, consultez la section Authentification et contrôle d'AWS KMSaccès du Guide du AWS Key Management Service développeur.

La manière de fournir cet accès à un rôle IAM dépend du fait que le compte propriétaire du rôle possède AWS KMS key également le rôle :

- Si le même compte possède la clé KMS et le rôle, un utilisateur du compte doit mettre à jour la politique de la clé.
- Si un compte possède la clé KMS et qu'un autre compte possède le rôle, un utilisateur du compte propriétaire de la clé doit autoriser l'accès entre comptes à la clé.

Cette rubrique décrit comment effectuer ces tâches pour un rôle IAM que vous avez créé pour récupérer des échantillons de données sensibles à partir d'objets S3. Il fournit également des exemples pour les deux scénarios. Pour plus d'informations sur l'autorisation d'accès aux services gérés par le client AWS KMS keys pour d'autres scénarios, consultez la section Authentification et contrôle d'accès AWS KMS dans le guide du AWS Key Management Service développeur.

Permettre à un même compte d'accéder à une clé gérée par le client

Si le même compte possède à la fois le rôle IAM AWS KMS key et le rôle IAM, un utilisateur du compte doit ajouter une déclaration à la politique de la clé. L'instruction supplémentaire doit autoriser le rôle IAM à déchiffrer les données à l'aide de la clé. Pour obtenir des informations détaillées sur la mise à jour d'une politique clé, consultez la section Modification d'une politique clé dans le Guide du AWS Key Management Service développeur.

Dans la déclaration :

- L'`Principal`élément doit spécifier le nom de ressource Amazon (ARN) du rôle IAM.
- Le `Action` tableau doit spécifier l'`kms:Decrypt`action. Il s'agit de la seule AWS KMS action que le rôle IAM doit être autorisé à effectuer pour déchiffrer un objet chiffré avec la clé.

Voici un exemple de l'instruction à ajouter à la politique pour une clé KMS.

```
{
    "Sid": "Allow the Macie reveal role to use the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/IAMRoleName"
    },
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": "*"
}
```

Dans l'exemple précédent :

- Le AWS champ de l'`Principal`élément indique l'ARN du rôle IAM dans le compte. Cela permet au rôle d'exécuter l'action spécifiée par la déclaration de politique. *123456789012* est un exemple d'ID de compte. Remplacez cette valeur par l'ID de compte du compte propriétaire du rôle et de la

clé KMS. *IAM RoleName* est un exemple de nom. Remplacez cette valeur par le nom du rôle IAM dans le compte.

- Le `Action` tableau indique l'action que le rôle IAM est autorisé à effectuer à l'aide de la clé KMS : déchiffrer le texte chiffré avec la clé.

L'endroit où vous ajoutez cette déclaration à une politique clé dépend de la structure et des éléments que la stratégie contient actuellement. Lorsque vous ajoutez l'instruction, assurez-vous que la syntaxe est valide. Les politiques clés utilisent le format JSON. Cela signifie que vous devez également ajouter une virgule avant ou après la déclaration, selon l'endroit où vous ajoutez la déclaration à la politique.

Autoriser l'accès entre comptes à une clé gérée par le client

Si un compte possède le AWS KMS key (propriétaire de la clé) et qu'un autre compte possède le rôle IAM (propriétaire du rôle), le propriétaire de la clé doit fournir au propriétaire du rôle un accès multicompte à la clé. L'un des moyens d'y parvenir est d'utiliser une subvention. Une subvention est un instrument de politique qui permet AWS aux principaux d'utiliser des clés KMS dans des opérations cryptographiques si les conditions spécifiées par la subvention sont remplies. Pour en savoir plus sur les subventions, consultez la section Subventions AWS KMS dans le guide du AWS Key Management Service développeur.

Avec cette approche, le propriétaire de la clé s'assure d'abord que la politique de la clé permet au propriétaire du rôle de créer une autorisation pour la clé. Le propriétaire du rôle crée ensuite une subvention pour la clé. La subvention délègue les autorisations pertinentes au rôle IAM dans leur compte. Cela permet au rôle de déchiffrer les objets S3 chiffrés avec la clé.

Étape 1 : Mettre à jour la politique clé

Dans la politique clé, le propriétaire de la clé doit s'assurer qu'elle inclut une déclaration qui permet au propriétaire du rôle de créer une autorisation pour le rôle IAM dans son compte (celui du propriétaire du rôle). Dans cette déclaration, l'`Principal`élément doit spécifier l'ARN du compte du propriétaire du rôle. Le `Action` tableau doit spécifier l'`kms:CreateGrant`action. Un `Condition` bloc peut filtrer l'accès à l'action spécifiée. Voici un exemple de cette déclaration dans la politique relative à une clé KMS.

```
{
    "Sid": "Allow a role in an account to create a grant",
    "Effect": "Allow",
```

```
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
    },
    "Action": [
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/IAMRoleName"
        },
        "ForAllValues:StringEquals": {
            "kms:GrantOperations": "Decrypt"
        }
    }
}
```

Dans l'exemple précédent :

- Le `AWS` champ de l'`Principal`élément indique l'ARN du compte du propriétaire du rôle. Il permet au compte d'effectuer l'action spécifiée par la déclaration de politique. *111122223333* est un exemple d'ID de compte. Remplacez cette valeur par l'ID du compte du propriétaire du rôle.
- Le `Action` tableau indique l'action que le propriétaire du rôle est autorisé à effectuer sur la clé KMS : créer une autorisation pour la clé.
- Le `Condition` bloc utilise les opérateurs de condition et les clés de condition suivantes pour filtrer l'accès à l'action que le propriétaire du rôle est autorisé à effectuer sur la clé KMS :
  - kms : GranteePrincipal — Cette condition permet au propriétaire du rôle de créer une subvention uniquement pour le bénéficiaire principal spécifié, qui est l'ARN du rôle IAM dans son compte. Dans cet ARN, *111122223333* est un exemple d'ID de compte. Remplacez cette valeur par l'ID du compte du propriétaire du rôle. *IAM RoleName* est un exemple de nom. Remplacez cette valeur par le nom du rôle IAM dans le compte du propriétaire du rôle.
  - kms : GrantOperations — Cette condition permet au propriétaire du rôle de créer une autorisation uniquement pour déléguer l'autorisation d'effectuer l'AWS KMS`Decrypt`action (déchiffrer le texte chiffré avec la clé). Cela empêche le propriétaire du rôle de créer des autorisations déléguant des autorisations pour effectuer d'autres actions sur la clé KMS. Il s'agit de la seule AWS KMS action que le rôle IAM doit être autorisé à effectuer pour déchiffrer un objet chiffré avec la clé. `Decrypt`

L'endroit où le propriétaire de la clé ajoute cette déclaration à la politique clé dépend de la structure et des éléments que la politique contient actuellement. Lorsque le propriétaire de la clé ajoute l'instruction, il doit s'assurer que la syntaxe est valide. Les politiques clés utilisent le format JSON. Cela signifie que le propriétaire de la clé doit également ajouter une virgule avant ou après l'instruction, selon l'endroit où il ajoute l'instruction à la politique. Pour obtenir des informations détaillées sur la mise à jour d'une politique clé, consultez la section Modification d'une politique clé dans le Guide du AWS Key Management Service développeur.

Étape 2 : Création d'une subvention

Une fois que le propriétaire de la clé a mis à jour la politique de clé si nécessaire, le propriétaire du rôle crée une autorisation pour la clé. La subvention délègue les autorisations pertinentes au rôle IAM dans leur compte (celui du propriétaire du rôle). Avant que le propriétaire du rôle ne crée la subvention, il doit vérifier qu'il est autorisé à effectuer l'`kms:CreateGrant`action. Cette action leur permet d'ajouter une subvention à une subvention existante gérée par le clientAWS KMS key.

Pour créer la subvention, le propriétaire du rôle peut utiliser le CreateGrantfonctionnement de l'AWS Key Management ServiceAPI. Lorsque le propriétaire du rôle crée la subvention, il doit spécifier les valeurs suivantes pour les paramètres requis :

- `KeyId`— L'ARN de la clé KMS. Pour un accès entre comptes à une clé KMS, cette valeur doit être un ARN. Il ne peut pas s'agir d'un identifiant clé.
- `GranteePrincipal`— L'ARN du rôle IAM dans leur compte. Cette valeur doit êtrearn:aws:iam::*111122223333*:role/*IAMRoleName*, où *111122223333* est l'ID de compte du propriétaire du rôle et *IAM RoleName* est le nom du rôle.
- `Operations`— L'action de AWS KMS déchiffrement (`Decrypt`). Il s'agit de la seule AWS KMS action que le rôle IAM doit être autorisé à effectuer pour déchiffrer un objet chiffré avec la clé KMS.

Si le propriétaire du rôle utilise le AWS Command Line Interface (AWS CLI), il peut exécuter la commande create-grant pour créer la subvention. L'exemple suivant montre comment procéder. L'exemple est formaté pour Microsoft Windows et utilise le caractère de continuation de ligne caret (^) pour améliorer la lisibilité.

```
C:\> aws kms create-grant ^
--key-id arn:aws:kms:us-east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab ^
--grantee-principal arn:aws:iam::111122223333:role/IAMRoleName ^
--operations "Decrypt"
```

Où :

- `key-id`spécifie l'ARN de la clé KMS à laquelle appliquer l'autorisation.
- `grantee-principal`spécifie l'ARN du rôle IAM autorisé à effectuer l'action spécifiée par la subvention. Cette valeur doit correspondre à l'ARN spécifié par la `kms:GranteePrincipal` condition dans la politique clé.
- `operations`spécifie l'action que l'autorisation autorise le principal spécifié à effectuer : déchiffrer le texte chiffré avec la clé.

Si la commande s'exécute correctement, vous recevez une sortie similaire à ce qui suit.

```
{
    "GrantToken": "<grant token>",
    "GrantId": "1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0dab1a59b2"
}
```

Où se `GrantToken` trouve une chaîne unique, non secrète, de longueur variable, codée en base64 qui représente la subvention créée et `GrantId` constitue l'identifiant unique de la subvention.

Configuration d'Amazon Macie pour récupérer et révéler des échantillons de données sensibles contenant des résultats

Vous pouvez éventuellement configurer et utiliser Amazon Macie pour récupérer et révéler des échantillons de données sensibles que Macie rapporte dans ses conclusions individuelles relatives aux données sensibles. Les exemples peuvent vous aider à vérifier la nature des données sensibles découvertes par Macie. Ils peuvent également vous aider à personnaliser votre enquête sur un objet ou un bucket Amazon Simple Storage Service (Amazon S3) concernés. Vous pouvez récupérer et révéler des échantillons de données sensibles dans tous les Régions AWS endroits où Macie est actuellement disponible, à l'exception des régions Asie-Pacifique (Osaka) et Israël (Tel Aviv).

Lorsque vous récupérez et révélez des échantillons de données sensibles pour une recherche, Macie utilise les données du résultat de découverte de données sensibles correspondant pour localiser les occurrences de données sensibles dans l'objet S3 concerné. Macie extrait ensuite des échantillons de ces occurrences de l'objet concerné. Macie chiffre les données extraites avec une clé AWS Key Management Service (AWS KMS) que vous spécifiez, stocke temporairement les données chiffrées dans un cache et renvoie les données dans vos résultats pour la recherche. Peu après l'extraction et le chiffrement, Macie supprime définitivement les données du cache, sauf si une conservation supplémentaire est temporairement requise pour résoudre un problème de fonctionnement.

Pour récupérer et révéler des échantillons de données sensibles à des fins de recherche, vous devez d'abord configurer et activer les paramètres de votre compte Macie. Vous devez également configurer les ressources de support et les autorisations pour votre compte. Les rubriques de cette section vous guident tout au long du processus de configuration de Macie pour récupérer et révéler des échantillons de données sensibles, et de gestion de l'état de la configuration de votre compte.

Rubriques

> **Tip**
>
> Pour obtenir des recommandations et des exemples de politiques que vous pouvez utiliser pour contrôler l'accès à cette fonctionnalité, consultez le billet de blog Comment utiliser Amazon Macie pour prévisualiser des données sensibles dans des compartiments S3 sur le AWS blog de sécurité.

Avant de commencer

Avant de configurer Amazon Macie pour récupérer et révéler des échantillons de données sensibles à des fins de recherche, effectuez les tâches suivantes pour vous assurer que vous disposez des ressources et des autorisations dont vous avez besoin.

Tâches

Ces tâches sont facultatives si vous avez déjà configuré Macie pour récupérer et révéler des échantillons de données sensibles et que vous souhaitez uniquement modifier vos paramètres de configuration.

Étape 1 : Configuration d'un référentiel pour les résultats de découverte de données sensibles

Lorsque vous récupérez et révélez des échantillons de données sensibles pour une recherche, Macie utilise les données du résultat de découverte de données sensibles correspondant pour localiser les occurrences de données sensibles dans l'objet S3 concerné. Il est donc important de vérifier que vous avez configuré un référentiel pour vos résultats de découverte de données sensibles. Sinon, Macie ne sera pas en mesure de localiser les échantillons de données sensibles que vous souhaitez récupérer et révéler.

Pour déterminer si vous avez configuré ce référentiel pour votre compte, vous pouvez utiliser la console Amazon Macie : choisissez Discovery results (sous Paramètres) dans le volet de navigation. Pour ce faire par programmation, utilisez le GetClassificationExportConfigurationfonctionnement de l'API Amazon Macie. Pour en savoir plus sur les résultats de découverte de données sensibles et sur la façon de configurer ce référentiel, consultezStockage et conservation des résultats de découverte de données sensibles.

Étape 2 : Déterminer comment accéder aux objets S3 concernés

Pour accéder aux objets S3 concernés et en extraire des échantillons de données sensibles, deux options s'offrent à vous. Vous pouvez configurer Macie pour qu'il utilise vos informations d'identification utilisateur AWS Identity and Access Management (IAM). Vous pouvez également configurer Macie pour qu'il assume un rôle IAM qui délègue l'accès à Macie. Vous pouvez utiliser l'une ou l'autre configuration avec n'importe quel type de compte Macie : un compte administrateur Macie délégué pour une organisation, un compte de membre Macie dans une organisation ou un compte Macie autonome. Avant de configurer les paramètres dans Macie, déterminez la méthode d'accès que vous souhaitez utiliser. Pour plus de détails sur les options et les exigences de chaque méthode, consultezOptions de configuration et exigences pour récupérer des échantillons de données sensibles contenant des résultats.

Si vous envisagez d'utiliser un rôle IAM, créez et configurez le rôle avant de configurer les paramètres dans Macie. Assurez-vous également que les politiques de confiance et d'autorisation relatives au rôle répondent à toutes les exigences pour que Macie assume le rôle. Si votre compte fait partie d'une organisation qui gère de manière centralisée plusieurs comptes Macie, contactez d'abord votre administrateur Macie pour déterminer si et comment configurer le rôle de votre compte.

Étape 3 : Configuration d'un AWS KMS key

Lorsque vous récupérez et révélez des échantillons de données sensibles pour une recherche, Macie chiffre les échantillons à l'aide d'une clé AWS Key Management Service (AWS KMS) que vous

spécifiez. Par conséquent, vous devez déterminer celui que AWS KMS key vous souhaitez utiliser pour chiffrer les échantillons. La clé peut être une clé KMS existante de votre propre compte ou une clé KMS existante détenue par un autre compte. Si vous souhaitez utiliser une clé détenue par un autre compte, obtenez le nom de ressource Amazon (ARN) de la clé. Vous devez spécifier cet ARN lorsque vous entrez les paramètres de configuration dans Macie.

La clé KMS doit être une clé de chiffrement symétrique gérée par le client. Il doit également s'agir d'une clé à région unique activée en même temps Région AWS que votre compte Macie. La clé KMS peut se trouver dans un magasin de clés externe. Cependant, la clé peut alors être plus lente et moins fiable qu'une clé entièrement gérée en interneAWS KMS. Si un problème de latence ou de disponibilité empêche Macie de chiffrer les échantillons de données sensibles que vous souhaitez récupérer et révéler, une erreur se produit et Macie ne renvoie aucun échantillon pour la recherche.

En outre, la politique de clé associée à la clé doit permettre aux principaux concernés (rôles IAM, utilisateurs IAM ouComptes AWS) d'effectuer les actions suivantes :

- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKey`

> **Important**
>
> Comme niveau supplémentaire de contrôle d'accès, nous vous recommandons de créer une clé KMS dédiée pour le chiffrement des échantillons de données sensibles récupérés, et de limiter l'utilisation de la clé aux seuls principaux qui doivent être autorisés à récupérer et à révéler des échantillons de données sensibles. Si un utilisateur n'est pas autorisé à effectuer les actions précédentes pour la clé, Macie rejette sa demande de récupération et de divulgation d'échantillons de données sensibles. Macie ne renvoie aucun échantillon pour la découverte.

Pour plus d'informations sur la création et la configuration des clés KMS, consultez la section Gestion des clés dans le Guide du AWS Key Management Service développeur. Pour plus d'informations sur l'utilisation de politiques clés pour gérer l'accès aux clés KMS, consultez la section Politiques clés du guide du AWS Key Management Service développeur. AWS KMS

Étape 4 : Vérifiez vos autorisations

Avant de configurer les paramètres dans Macie, vérifiez également que vous disposez des autorisations nécessaires. Pour vérifier vos autorisations, utilisez AWS Identity and Access Management (IAM) pour examiner les politiques IAM associées à votre identité IAM. Comparez ensuite les informations contenues dans ces politiques à la liste suivante des actions que vous devez être autorisé à effectuer.

Amazon Macie

Pour Macie, vérifiez que vous êtes autorisé à effectuer les actions suivantes :

- `macie2:GetMacieSession`
- `macie2:UpdateRevealConfiguration`

La première action vous permet d'accéder à votre compte Macie. La deuxième action vous permet de modifier vos paramètres de configuration pour récupérer et révéler des échantillons de données sensibles. Cela inclut l'activation et la désactivation de la configuration de votre compte.

Vérifiez éventuellement que vous êtes également autorisé à effectuer l'`macie2:GetRevealConfiguration`action. Cette action vous permet de récupérer vos paramètres de configuration actuels et l'état actuel de la configuration de votre compte.

AWS KMS

Si vous prévoyez d'utiliser la console Amazon Macie pour entrer les paramètres de configuration, vérifiez également que vous êtes autorisé à effectuer les actions suivantes AWS Key Management Service (AWS KMS) :

- `kms:DescribeKey`
- `kms:ListAliases`

Ces actions vous permettent de récupérer des informations AWS KMS keys relatives à votre compte. Vous pouvez ensuite choisir l'une de ces touches lorsque vous entrez les paramètres.

IAM

Si vous envisagez de configurer Macie pour qu'il assume un rôle IAM afin de récupérer et de révéler des échantillons de données sensibles, vérifiez également que vous êtes autorisé à effectuer l'action IAM suivante :. `iam:PassRole` Cette action vous permet de passer le rôle à Macie, qui à son tour permet à Macie d'assumer le rôle. Lorsque vous entrez les paramètres de configuration de votre compte, Macie peut également vérifier que le rôle existe dans votre compte et qu'il est correctement configuré.

Si vous n'êtes pas autorisé à effectuer les actions requises, demandez de l'aide à votre AWS administrateur.

Configuration et activation des paramètres Amazon Macie

Après avoir vérifié que vous disposez des ressources et des autorisations nécessaires, vous pouvez configurer les paramètres dans Amazon Macie et activer la configuration de votre compte.

Si votre compte fait partie d'une organisation qui gère de manière centralisée plusieurs comptes Macie, notez ce qui suit avant de configurer ou de modifier ultérieurement les paramètres de votre compte :

- Si vous avez un compte membre, contactez votre administrateur Macie pour déterminer si et comment configurer les paramètres de votre compte. Votre administrateur Macie peut vous aider à déterminer les paramètres de configuration appropriés pour votre compte.
- Si vous disposez d'un compte administrateur Macie et que vous modifiez les paramètres d'accès aux objets S3 concernés, vos modifications peuvent affecter d'autres comptes et ressources de votre organisation. Cela dépend si Macie est actuellement configuré pour assumer un rôle AWS Identity and Access Management (IAM) afin de récupérer des échantillons de données sensibles. Si tel est le cas et que vous reconfigurez Macie pour utiliser les informations d'identification utilisateur IAM, Macie supprime définitivement les paramètres existants pour le rôle IAM, à savoir le nom du rôle et l'ID externe de votre configuration. Si votre organisation choisit par la suite d'utiliser à nouveau les rôles IAM, vous devrez spécifier un nouvel identifiant externe dans la politique de confiance pour le rôle dans chaque compte membre applicable.

Pour plus de détails sur les options de configuration pour l'un ou l'autre type de compte, consultezOptions de configuration et exigences pour récupérer des échantillons de données sensibles contenant des résultats.

Pour configurer les paramètres dans Macie et activer la configuration de votre compte, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie.

Console

Suivez ces étapes pour configurer et activer les paramètres à l'aide de la console Amazon Macie.

Pour configurer et activer les paramètres Macie

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.

2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez configurer et permettez à Macie de récupérer et de révéler des échantillons de données sensibles.
3. Dans le volet de navigation, sous Paramètres, sélectionnez Afficher les échantillons.
4. Dans la section Settings (Paramètres), choisissez Edit (Modifier).
5. Pour Status (Statut), choisissez Enabled (Activé).
6. Sous Accès, spécifiez la méthode d'accès et les paramètres que vous souhaitez utiliser lors de la récupération d'échantillons de données sensibles à partir des objets S3 concernés :

   - Pour utiliser un rôle IAM qui délègue l'accès à Macie, choisissez Assumer un rôle IAM. Si vous choisissez cette option, Macie récupère les échantillons en assumant le rôle IAM que vous avez créé et configuré dans votre. Compte AWS Dans le champ Nom du rôle, entrez le nom du rôle.
   - Pour utiliser les informations d'identification de l'utilisateur IAM qui demande les échantillons, choisissez Utiliser les informations d'identification de l'utilisateur IAM. Si vous choisissez cette option, chaque utilisateur de votre compte utilise son identité IAM individuelle pour récupérer les échantillons.
7. Sous Chiffrement, spécifiez AWS KMS key celui que vous souhaitez utiliser pour chiffrer les échantillons de données sensibles récupérés :

   - Pour utiliser une clé KMS de votre propre compte, choisissez Sélectionner une clé de votre compte. Ensuite, dans la AWS KMS keyliste, choisissez la clé à utiliser. La liste affiche les clés KMS de chiffrement symétriques existantes pour votre compte.
   - Pour utiliser une clé KMS détenue par un autre compte, choisissez Enter the ARN of a key from another account. Ensuite, dans le champ AWS KMS keyARN, entrez le nom de ressource Amazon (ARN) de la clé à utiliser, par exemple. **`arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`**
8. Lorsque vous avez fini de saisir les paramètres, choisissez Enregistrer.

Macie teste les paramètres et vérifie qu'ils sont corrects. Si vous avez configuré Macie pour qu'il assume un rôle IAM, Macie vérifie également que le rôle existe dans votre compte et que les politiques de confiance et d'autorisation sont correctement configurées. En cas de problème, Macie affiche un message décrivant le problème.

Pour résoudre un problème lié auAWS KMS key, reportez-vous aux exigences de la rubrique précédente et spécifiez une clé KMS répondant à ces exigences. Pour résoudre un problème lié

au rôle IAM, commencez par vérifier que vous avez saisi le nom de rôle correct. Si le nom est correct, assurez-vous que les politiques du rôle répondent à toutes les exigences pour que Macie assume le rôle. Pour plus de détails, voirConfiguration d'un rôle IAM pour accéder aux objets S3 concernés. Une fois les problèmes résolus, vous pouvez enregistrer et activer les paramètres.

> **Note**
>
> Si vous êtes l'administrateur Macie d'une organisation et que vous avez configuré Macie pour qu'il assume un rôle IAM, Macie génère et affiche un identifiant externe après avoir enregistré les paramètres de votre compte. Notez cet identifiant. La politique de confiance pour le rôle IAM dans chacun de vos comptes membres applicables doit spécifier cet ID. Dans le cas contraire, vous ne pourrez pas récupérer d'échantillons de données sensibles à partir d'objets S3 détenus par les comptes.

API

Pour configurer et activer les paramètres par programmation, utilisez l'UpdateRevealConfigurationAPI Amazon Macie. Dans votre demande, spécifiez les valeurs appropriées pour les paramètres pris en charge :

- Pour les `retrievalConfiguration` paramètres, spécifiez la méthode d'accès et les paramètres que vous souhaitez utiliser lors de la récupération d'échantillons de données sensibles à partir des objets S3 concernés :
  - Pour assumer un rôle IAM qui délègue l'accès à Macie, spécifiez `ASSUME_ROLE` le `retrievalMode` paramètre et le nom du rôle pour le `roleName` paramètre. Si vous spécifiez ces paramètres, Macie récupère les exemples en assumant le rôle IAM que vous avez créé et configuré dans votre. Compte AWS
  - Pour utiliser les informations d'identification de l'utilisateur IAM qui demande les échantillons, spécifiez `CALLER_CREDENTIALS` le `retrievalMode` paramètre. Si vous spécifiez ce paramètre, chaque utilisateur de votre compte utilise son identité IAM individuelle pour récupérer les échantillons.

> **Important**
>
> Si vous ne spécifiez aucune valeur pour ces paramètres, Macie définit la méthode d'accès (`retrievalMode`) sur`CALLER_CREDENTIALS`. Si Macie est actuellement configuré pour utiliser un rôle IAM pour récupérer les échantillons, Macie supprime

également définitivement le nom du rôle actuel et l'ID externe de votre configuration. Pour conserver ces paramètres pour une configuration existante, incluez-les `retrievalConfiguration` dans votre demande et spécifiez vos paramètres actuels pour ces paramètres. Pour récupérer vos paramètres actuels, utilisez l'GetRevealConfigurationopération ou, si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la get-reveal-configurationcommande.

- Pour le `kmsKeyId` paramètre, spécifiez celui AWS KMS key que vous souhaitez utiliser pour chiffrer les échantillons de données sensibles récupérés :
  - Pour utiliser une clé KMS depuis votre propre compte, spécifiez le nom de ressource Amazon (ARN), l'ID ou l'alias de la clé. Si vous spécifiez un alias, incluez le `alias/` préfixe, par exemple,. `alias/ExampleAlias`
  - Pour utiliser une clé KMS détenue par un autre compte, spécifiez l'ARN de la clé, par exemple,. `arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` Ou spécifiez l'ARN de l'alias de la clé, par exemple,. `arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias`
- Pour le `status` paramètre, spécifiez `ENABLED` d'activer la configuration pour votre compte Macie.

Dans votre demande, assurez-vous également de spécifier la configuration Région AWS dans laquelle vous souhaitez activer et utiliser.

Pour configurer et activer les paramètres à l'aide deAWS CLI, exécutez la update-reveal-configurationcommande et spécifiez les valeurs appropriées pour les paramètres pris en charge. Par exemple, si vous utilisez AWS CLI le sous Microsoft Windows, exécutez la commande suivante :

```
C:\> aws macie2 update-reveal-configuration ^
--region us-east-1 ^
--configuration={\"kmsKeyId\":\"arn:aws:kms:us-east-1:111122223333:alias/
ExampleAlias\",\"status\":\"ENABLED\"} ^
--retrievalConfiguration={\"retrievalMode\":\"ASSUME_ROLE\",\"roleName\":
\"MacieRevealRole\"}
```

Où :

- *us-east-1* est la région dans laquelle activer et utiliser la configuration. Dans cet exemple, la région de l'est des États-Unis (Virginie du Nord).
- *arn:aws:kms:us-east- ExampleAlias 1:111122223333:alias/* est l'ARN de l'alias à utiliser. AWS KMS key Dans cet exemple, la clé appartient à un autre compte.
- ENABLEDest l'état de la configuration.
- *ASSUME_ROLE* est la méthode d'accès à utiliser. Dans cet exemple, assumez le rôle IAM spécifié.
- *MacieRevealRole*est le nom du rôle IAM que Macie doit assumer lors de la récupération d'échantillons de données sensibles.

L'exemple précédent utilise le caractère de continuation de ligne caret (^) pour améliorer la lisibilité.

Lorsque vous soumettez votre demande, Macie teste les paramètres. Si vous avez configuré Macie pour qu'il assume un rôle IAM, Macie vérifie également que le rôle existe dans votre compte et que les politiques de confiance et d'autorisation sont correctement configurées. En cas de problème, votre demande échoue et Macie renvoie un message décrivant le problème. Pour résoudre un problème lié auAWS KMS key, reportez-vous aux exigences de la rubrique précédente et spécifiez une clé KMS répondant à ces exigences. Pour résoudre un problème lié au rôle IAM, commencez par vérifier que vous avez spécifié le nom de rôle correct. Si le nom est correct, assurez-vous que les politiques du rôle répondent à toutes les exigences pour que Macie assume le rôle. Pour plus de détails, voirConfiguration d'un rôle IAM pour accéder aux objets S3 concernés. Une fois le problème résolu, soumettez à nouveau votre demande.

Si votre demande aboutit, Macie active la configuration de votre compte dans la région spécifiée et vous recevez un résultat similaire à ce qui suit.

```
{
  "configuration": {
    "kmsKeyId": "arn:aws:kms:us-east-1:111122223333:alias/ExampleAlias",
    "status": "ENABLED"
  },
  "retrievalConfiguration": {
    "externalId": "o2vee30hs31642lexample",
    "retrievalMode": "ASSUME_ROLE",
    "roleName": "MacieRevealRole"
  }
}
```

Where `kmsKeyId` indique le code AWS KMS key à utiliser pour chiffrer les échantillons de données sensibles récupérés et `status` indique l'état de la configuration de votre compte Macie. Les `retrievalConfiguration` valeurs indiquent la méthode d'accès et les paramètres à utiliser lors de la récupération des échantillons.

> **Note**
>
> Si vous êtes l'administrateur Macie d'une organisation et que vous avez configuré Macie pour qu'il assume un rôle IAM, notez l'ID externe (`externalId`) dans la réponse. La politique de confiance pour le rôle IAM dans chacun de vos comptes membres applicables doit spécifier cet ID. Dans le cas contraire, vous ne pourrez pas récupérer d'échantillons de données sensibles à partir des objets S3 concernés détenus par les comptes.

Pour vérifier ultérieurement les paramètres ou l'état de la configuration de votre compte, utilisez l'GetRevealConfigurationopération ou, pour leAWS CLI, exécutez la get-reveal-configurationcommande.

Désactivation des paramètres Amazon Macie

Vous pouvez désactiver les paramètres de configuration de votre compte Amazon Macie à tout moment. Si vous désactivez la configuration, Macie conserve le paramètre qui indique lequel utiliser AWS KMS key pour chiffrer les échantillons de données sensibles récupérés. Macie supprime définitivement les paramètres d'accès Amazon S3 pour la configuration.

> **Warning**
>
> Lorsque vous désactivez les paramètres de configuration de votre compte Macie, vous supprimez également définitivement les paramètres actuels qui spécifient comment accéder aux objets S3 concernés. Si Macie est actuellement configuré pour accéder aux objets concernés en assumant un rôle AWS Identity and Access Management (IAM), cela inclut : le nom du rôle et l'ID externe généré par Macie pour la configuration. Ces paramètres ne peuvent pas être restaurés après leur suppression.

Pour désactiver les paramètres de configuration de votre compte Macie, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie.

Console

Suivez ces étapes pour désactiver les paramètres de configuration de votre compte à l'aide de la console Amazon Macie.

Pour désactiver les paramètres Macie

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez désactiver les paramètres de configuration de votre compte Macie.
3. Dans le volet de navigation, sous Paramètres, sélectionnez Afficher les échantillons.
4. Dans la section Settings (Paramètres), choisissez Edit (Modifier).
5. Dans le champ État, choisissez Désactiver.
6. Choisissez Enregistrer.

API

Pour désactiver les paramètres de configuration par programmation, utilisez l'UpdateRevealConfigurationAPI Amazon Macie. Dans votre demande, assurez-vous de spécifier la configuration Région AWS dans laquelle vous souhaitez désactiver la configuration. Pour le paramètre `status`, spécifiez `DISABLED`.

Pour désactiver les paramètres de configuration à l'aide de AWS Command Line Interface (AWS CLI), exécutez la update-reveal-configurationcommande. Utilisez le `region` paramètre pour spécifier la région dans laquelle vous souhaitez désactiver la configuration. Pour le paramètre `status`, spécifiez `DISABLED`. Par exemple, si vous utilisez AWS CLI le sous Microsoft Windows, exécutez la commande suivante :

```
C:\> aws macie2 update-reveal-configuration --region us-east-1 --
configuration={\"status\":\"DISABLED\"}
```

Où :

- *`us-east-1`* est la région dans laquelle la configuration doit être désactivée. Dans cet exemple, la région de l'est des États-Unis (Virginie du Nord).
- `DISABLED`est le nouveau statut de la configuration.

Si votre demande aboutit, Macie désactive la configuration de votre compte dans la région spécifiée et vous recevez un résultat similaire à ce qui suit.

```
{
    "configuration": {
        "status": "DISABLED"
    }
}
```

Où `status` est le nouveau statut de la configuration de votre compte Macie.

Si Macie a été configuré pour assumer un rôle IAM afin de récupérer des échantillons de données sensibles, vous pouvez éventuellement supprimer le rôle et la politique d'autorisation du rôle. Macie ne supprime pas ces ressources lorsque vous désactivez les paramètres de configuration de votre compte. De plus, Macie n'utilise pas ces ressources pour effectuer d'autres tâches pour votre compte. Pour supprimer le rôle et sa politique d'autorisations, vous pouvez utiliser la console IAM ou l'API IAM. Pour plus d'informations, consultez la section Suppression de rôles dans le guide de AWS Identity and Access Management l'utilisateur.

Extraction et divulgation d'échantillons de données sensibles accompagnés de résultats

En utilisant Amazon Macie, vous pouvez récupérer et révéler des échantillons de données sensibles que Macie rapporte dans ses conclusions individuelles relatives aux données sensibles. Cela inclut les données sensibles détectées par Macie à l'aide d'identifiants de données gérés et les données qui répondent aux critères des identifiants de données personnalisés. Les exemples peuvent vous aider à vérifier la nature des données sensibles découvertes par Macie. Ils peuvent également vous aider à personnaliser votre enquête sur un objet ou un bucket Amazon Simple Storage Service (Amazon S3) concernés. Vous pouvez récupérer et révéler des échantillons de données sensibles dans tous les Régions AWS endroits où Macie est actuellement disponible, à l'exception des régions Asie-Pacifique (Osaka) et Israël (Tel Aviv).

Si vous récupérez et révélez des échantillons de données sensibles pour une découverte, Macie utilise les données du résultat de découverte de données sensibles correspondant pour localiser les 1 à 10 premières occurrences de données sensibles signalées par la découverte. Macie extrait ensuite les 1 à 128 premiers caractères de chaque occurrence de l'objet S3 concerné. Si une découverte fait état de plusieurs types de données sensibles, Macie le fait pour un maximum de 100 types de données sensibles signalés par la découverte.

Lorsque Macie extrait des données sensibles d'un objet S3 concerné, Macie chiffre les données avec une clé AWS Key Management Service (AWS KMS) que vous spécifiez, stocke temporairement les données chiffrées dans un cache et renvoie les données dans vos résultats pour la recherche. Peu après l'extraction et le chiffrement, Macie supprime définitivement les données du cache, sauf si une conservation supplémentaire est temporairement requise pour résoudre un problème de fonctionnement.

Si vous choisissez de récupérer et de révéler des échantillons de données sensibles pour une nouvelle recherche, Macie répète le processus de localisation, d'extraction, de chiffrement, de stockage et finalement de suppression des échantillons.

Pour découvrir comment récupérer et révéler des échantillons de données sensibles à l'aide de la console Amazon Macie, regardez la vidéo suivante : Extraction et divulgation d'échantillons de données sensibles avec Amazon Macie.

Rubriques

Avant de commencer

Avant de pouvoir récupérer et révéler des échantillons de données sensibles à des fins de recherche, vous devez configurer et activer les paramètres de votre compte Amazon Macie. Vous devez également travailler avec votre AWS administrateur pour vérifier que vous disposez des autorisations et des ressources dont vous avez besoin.

Lorsque vous récupérez et révélez des échantillons de données sensibles à des fins de recherche, Macie exécute une série de tâches pour localiser, récupérer, chiffrer et révéler les échantillons. Macie n'utilise pas le rôle lié au service Macie pour votre compte pour effectuer ces tâches. Au lieu de cela, vous utilisez votre identité AWS Identity and Access Management (IAM) ou vous autorisez Macie à assumer un rôle IAM dans votre compte.

Pour récupérer et révéler des échantillons de données sensibles pour une découverte, vous devez avoir accès à la découverte de données sensibles, au résultat de découverte de données sensibles correspondant et à celui AWS KMS key que vous avez configuré Macie pour chiffrer les échantillons de données sensibles. En outre, vous ou le rôle IAM devez être autorisé à accéder au compartiment

S3 et à l'objet S3 concernés. Vous ou le rôle devez également être autorisé à utiliser celui AWS KMS key qui a été utilisé pour chiffrer l'objet concerné, le cas échéant. Si des politiques IAM, des politiques de ressources ou d'autres paramètres d'autorisation refusent l'accès requis, une erreur se produit et Macie ne renvoie aucun échantillon pour la recherche.

Vous devez également être autorisé à effectuer les actions Macie suivantes :

- `macie2:GetMacieSession`
- `macie2:GetFindings`
- `macie2:ListFindings`
- `macie2:GetSensitiveDataOccurrences`

Les trois premières actions vous permettent d'accéder à votre compte Macie et de récupérer le détail des résultats. La dernière action vous permet de récupérer et de révéler des échantillons de données sensibles pour les résultats.

Pour utiliser la console Amazon Macie afin de récupérer et de révéler des échantillons de données sensibles, vous devez également être autorisé à effectuer l'action suivante : `macie2:GetSensitiveDataOccurrencesAvailability` Cette action vous permet de déterminer si des échantillons sont disponibles pour des résultats individuels. Vous n'avez pas besoin d'autorisation pour effectuer cette action afin de récupérer et de révéler des échantillons par programmation. Toutefois, l'obtention de cette autorisation peut rationaliser la récupération des échantillons.

Si vous êtes l'administrateur Macie délégué d'une organisation et que vous avez configuré Macie pour assumer un rôle IAM afin de récupérer des échantillons de données sensibles, vous devez également être autorisé à effectuer l'action suivante : `macie2:GetMember` Cette action vous permet de récupérer des informations sur l'association entre votre compte et un compte concerné. Cela permet à Macie de vérifier que vous êtes actuellement l'administrateur Macie du compte concerné.

Si vous n'êtes pas autorisé à effectuer les actions requises ou à accéder aux données et aux ressources requises, demandez de l'aide à votre AWS administrateur.

Déterminer si des échantillons de données sensibles sont disponibles pour une recherche

Pour récupérer et révéler des échantillons de données sensibles en vue d'une découverte, celle-ci doit répondre à certains critères. Il doit inclure des données de localisation pour des occurrences spécifiques de données sensibles. En outre, il doit spécifier l'emplacement d'un résultat de

découverte de données sensibles valide correspondant. Le résultat de la découverte de données sensibles doit être stocké au même Région AWS endroit que le résultat. Si vous avez configuré Amazon Macie pour accéder aux objets S3 concernés en assumant un rôle AWS Identity and Access Management (IAM), le résultat de la découverte de données sensibles doit également être stocké dans un objet S3 que Macie a signé avec un code d'authentification de message basé sur le hachage (HMAC). AWS KMS key

L'objet S3 concerné doit également répondre à certains critères. Le type MIME de l'objet doit être l'un des suivants :

- application/avro, pour un fichier conteneur d'objets Apache Avro (.avro)
- application/gzip, pour un fichier d'archive compressé GNU Zip (.gz ou .gzip)
- application/json, pour un fichier JSON ou JSON Lines (.json ou .jsonl)
- application/parquet, pour un fichier Apache Parquet (.parquet)
- application/vnd.openxmlformats-officedocument.spreadsheetml.sheet, pour un classeur Microsoft Excel (.xlsx)
- application/zip, pour un fichier d'archive compressé ZIP (.zip)
- text/csv, pour un fichier CSV (.csv)
- text/plain, pour un fichier texte non binaire autre qu'un fichier CSV, JSON, JSON Lines ou TSV
- text/tab-separated-values, pour un fichier TSV (.tsv)

En outre, le contenu de l'objet S3 doit être le même que lors de la création de la recherche. Macie vérifie la balise d'entité (ETag) de l'objet pour déterminer si elle correspond à l'ETag spécifiée par le résultat. En outre, la taille de stockage de l'objet ne peut pas dépasser le quota de taille applicable pour récupérer et révéler des échantillons de données sensibles. Pour obtenir la liste des quotas applicables, voirQuotas Amazon Macie.

Si un résultat et l'objet S3 concerné répondent aux critères précédents, des échantillons de données sensibles sont disponibles pour le résultat. Vous pouvez éventuellement déterminer si c'est le cas pour une découverte particulière avant d'essayer de récupérer et de révéler des échantillons correspondant à cette découverte.

Pour déterminer si des échantillons de données sensibles sont disponibles pour une recherche

Vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie pour déterminer si des échantillons de données sensibles sont disponibles pour une recherche.

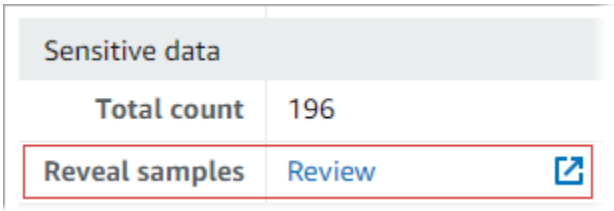
Console

Suivez ces étapes sur la console Amazon Macie pour déterminer si des échantillons de données sensibles sont disponibles pour une recherche.

Pour déterminer si des échantillons sont disponibles pour une recherche

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Conclusions.
3. Sur la page Résultats, sélectionnez le résultat. Le panneau des détails affiche des informations relatives au résultat.
4. Dans le panneau de détails, accédez à la section Données sensibles. Reportez-vous ensuite au champ Reveal samples.

   Si des échantillons de données sensibles sont disponibles pour la recherche, un lien de révision apparaît dans le champ, comme illustré dans l'image suivante.



   Si des échantillons de données sensibles ne sont pas disponibles pour la recherche, le champ Afficher les échantillons affiche un texte indiquant pourquoi :

   - Le compte ne fait pas partie de l'organisation : vous n'êtes pas autorisé à accéder à l'objet S3 concerné à l'aide de Macie. Le compte concerné ne fait actuellement pas partie de votre organisation. Ou bien le compte fait partie de votre organisation, mais Macie n'est actuellement pas activé pour le compte. Région AWS
   - Résultat de classification non valide : il n'existe aucun résultat de découverte de données sensibles correspondant à la recherche. Ou le résultat de découverte de données sensibles correspondant n'est pas disponible actuellement Région AWS, est mal formé ou endommagé, ou utilise un format de stockage non pris en charge. Macie ne peut pas vérifier l'emplacement des données sensibles à récupérer.
   - Signature de résultat non valide — Le résultat de découverte de données sensibles correspondant est stocké dans un objet S3 qui n'a pas été signé par Macie. Macie ne peut pas vérifier l'intégrité et l'authenticité du résultat de la découverte de données sensibles. Macie ne peut donc pas vérifier l'emplacement des données sensibles à récupérer.

- Rôle de membre trop permissif — La politique de confiance ou d'autorisation pour le rôle IAM dans le compte de membre concerné ne répond pas aux exigences de Macie en matière de restriction de l'accès au rôle. Ou bien, la politique de confiance du rôle ne spécifie pas l'identifiant externe approprié pour votre organisation. Macie ne peut pas assumer le rôle de récupérer les données sensibles.
- GetMember Autorisation manquante — Vous n'êtes pas autorisé à récupérer les informations relatives à l'association entre votre compte et le compte concerné. Macie ne peut pas déterminer si vous êtes autorisé à accéder à l'objet S3 concerné en tant qu'administrateur Macie délégué pour le compte concerné.
- L'objet dépasse le quota de taille : la taille de stockage de l'objet S3 concerné dépasse le quota de taille pour récupérer et révéler des échantillons de données sensibles à partir de ce type de fichier.
- Objet non disponible : l'objet S3 concerné n'est pas disponible. L'objet a été renommé, déplacé ou supprimé, ou son contenu a été modifié après que Macie a créé la recherche. Ou bien l'objet est chiffré avec un AWS KMS key code actuellement désactivé.
- Résultat non signé — Le résultat de découverte de données sensibles correspondant est stocké dans un objet S3 qui n'a pas été signé. Macie ne peut pas vérifier l'intégrité et l'authenticité du résultat de la découverte de données sensibles. Macie ne peut donc pas vérifier l'emplacement des données sensibles à récupérer.
- Rôle trop permissif : votre compte est configuré pour récupérer des occurrences de données sensibles en utilisant un rôle IAM dont la politique de confiance ou d'autorisation ne répond pas aux exigences de Macie en matière de restriction de l'accès au rôle. Macie ne peut pas assumer le rôle de récupérer les données sensibles.
- Type d'objet non pris en charge — L'objet S3 concerné utilise un format de fichier ou de stockage que Macie ne prend pas en charge pour récupérer et révéler des échantillons de données sensibles. Le type MIME de l'objet S3 concerné ne figure pas parmi les valeurs de la liste précédente.

En cas de problème lié au résultat de découverte de données sensibles pour la recherche, les informations contenues dans le champ Emplacement détaillé des résultats de la recherche peuvent vous aider à étudier le problème. Ce champ indique le chemin d'origine vers le résultat dans Amazon S3. Pour étudier un problème lié à un rôle IAM, assurez-vous que les politiques du rôle répondent à toutes les exigences permettant à Macie d'assumer ce rôle. Pour plus de détails, voirConfiguration d'un rôle IAM pour accéder aux objets S3 concernés.

API

Pour déterminer par programmation si des échantillons de données sensibles sont disponibles pour une recherche, utilisez le GetSensitiveDataOccurrencesAvailabilityfonctionnement de l'API Amazon Macie. Lorsque vous soumettez votre demande, utilisez le `findingId` paramètre pour spécifier l'identifiant unique de la recherche. Pour obtenir cet identifiant, vous pouvez utiliser l'ListFindingsopération.

Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande get-sensitive-data-occurrences-availability et utilisez le `finding-id` paramètre pour spécifier l'identifiant unique de la recherche. Pour obtenir cet identifiant, vous pouvez exécuter la commande list-findings.

Si votre demande aboutit et que des échantillons sont disponibles pour la recherche, vous recevez un résultat similaire à ce qui suit :

```
{
    "code": "AVAILABLE",
    "reasons": []
}
```

Si votre demande aboutit et qu'aucun échantillon n'est disponible pour la recherche, la valeur du `code` champ est `UNAVAILABLE` et le `reasons` tableau indique pourquoi. Par exemple :

```
{
    "code": "UNAVAILABLE",
    "reasons": [
        "UNSUPPORTED_OBJECT_TYPE"
    ]
}
```

En cas de problème lié au résultat de découverte de données sensibles lié à la découverte, les informations contenues dans le `classificationDetails.detailedResultsLocation` champ de la recherche peuvent vous aider à étudier le problème. Ce champ indique le chemin d'origine vers le résultat dans Amazon S3. Pour étudier un problème lié à un rôle IAM, assurez-vous que les politiques du rôle répondent à toutes les exigences permettant à Macie d'assumer ce rôle. Pour plus de détails, voirConfiguration d'un rôle IAM pour accéder aux objets S3 concernés.

Extraction et divulgation d'échantillons de données sensibles à des fins de recherche

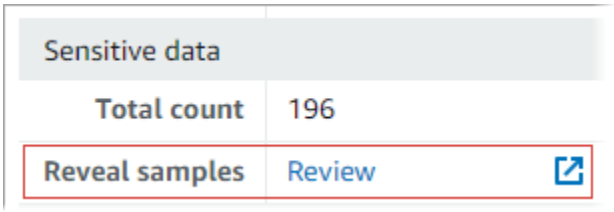
Pour récupérer et révéler des échantillons de données sensibles à des fins de recherche, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie.

Console

Suivez ces étapes pour récupérer et révéler des échantillons de données sensibles à des fins de recherche à l'aide de la console Amazon Macie.

Pour récupérer et révéler des échantillons de données sensibles en vue d'une découverte

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Conclusions.
3. Sur la page Résultats, sélectionnez le résultat. Le panneau des détails affiche des informations relatives au résultat.
4. Dans le panneau de détails, accédez à la section Données sensibles. Ensuite, dans le champ Reveal samples, sélectionnez Review :



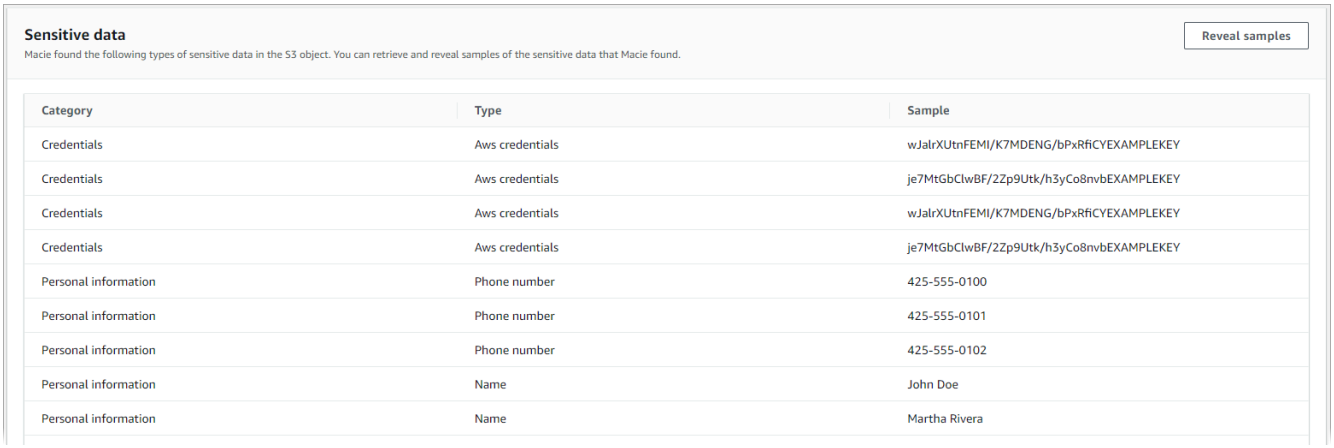
> **Note**
>
> Si le lien Révision n'apparaît pas dans le champ Afficher les échantillons, cela signifie que les échantillons de données sensibles ne sont pas disponibles pour la recherche. Pour savoir pourquoi c'est le cas, consultez la rubrique précédente.

Une fois que vous avez choisi Réviser, Macie affiche une page résumant les principaux détails du résultat. Les détails incluent les catégories, les types et le nombre d'occurrences de données sensibles que Macie a trouvées dans l'objet S3 concerné.

5. Dans la section Données sensibles de la page, sélectionnez Afficher les échantillons. Macie récupère et dévoile ensuite des échantillons des 1 à 10 premières occurrences de données sensibles signalées par la découverte. Chaque échantillon contient les 1 à 128

premiers caractères d'une occurrence de données sensibles. Plusieurs minutes peuvent être nécessaires pour récupérer et révéler les échantillons.

Si la découverte fait état de plusieurs types de données sensibles, Macie récupère et dévoile des échantillons pour un maximum de 100 types. Par exemple, l'image suivante montre des exemples qui couvrent plusieurs catégories et types de données sensibles : informations AWS d'identification, numéros de téléphone américains et noms de personnes.



Les échantillons sont d'abord organisés par catégorie de données sensibles, puis par type de données sensibles.

API

Pour récupérer et révéler des échantillons de données sensibles à des fins de recherche par programmation, utilisez le GetSensitiveDataOccurrencesfonctionnement de l'API Amazon Macie. Lorsque vous soumettez votre demande, utilisez le `findingId` paramètre pour spécifier l'identifiant unique de la recherche. Pour obtenir cet identifiant, vous pouvez utiliser l'ListFindingsopération.

Pour récupérer et révéler des échantillons de données sensibles à l'aide de AWS Command Line Interface (AWS CLI), exécutez la get-sensitive-data-occurrencescommande et utilisez le `finding-id` paramètre pour spécifier l'identifiant unique de la recherche. Par exemple :

```
C:\> aws macie2 get-sensitive-data-occurrences --finding-id
 "1f1c2d74db5d8caa76859ec52example"
```

Où *1f1c2d74db5d8caa76859ec52example* est l'identifiant unique du résultat. Pour obtenir cet identifiant à l'aide de AWS CLI, vous pouvez exécuter la commande list-findings.

Si votre demande aboutit, Macie commence à traiter votre demande et vous recevez un résultat similaire à ce qui suit :

```
{
    "status": "PROCESSING"
}
```

Le traitement de votre demande peut prendre plusieurs minutes. Dans quelques minutes, soumettez à nouveau votre demande.

Si Macie peut localiser, récupérer et chiffrer les échantillons de données sensibles, Macie renvoie les échantillons sur une carte. `sensitiveDataOccurrences` La carte indique 1 à 100 types de données sensibles signalées par la découverte et, pour chaque type, 1 à 10 échantillons. Chaque échantillon contient les 1 à 128 premiers caractères d'une occurrence de données sensibles signalées par le résultat.

Sur la carte, chaque clé est l'ID de l'identifiant des données gérées qui a détecté les données sensibles, ou le nom et l'identifiant unique de l'identifiant de données personnalisé qui a détecté les données sensibles. Les valeurs sont des exemples pour l'identifiant de données gérées ou l'identifiant de données personnalisé spécifié. Par exemple, la réponse suivante fournit trois échantillons de noms de personnes et deux échantillons de clés d'accès AWS secrètes détectées par des identifiants de données gérés (`NAME`et`AWS_CREDENTIALS`, respectivement).

```
{
    "sensitiveDataOccurrences": {
        "NAME": [
            {
                "value": "Akua Mansa"
            },
            {
                "value": "John Doe"
            },
            {
                "value": "Martha Rivera"
            }
        ],
        "AWS_CREDENTIALS": [
            {
                "value": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
            },
            {
```

```
                "value": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
            }
        ]
    },
    "status": "SUCCESS"
}
```

Si votre demande aboutit mais que les échantillons de données sensibles ne sont pas disponibles pour la recherche, vous recevez un `UnprocessableEntityException` message indiquant pourquoi les échantillons ne sont pas disponibles. Par exemple :

```
{
    "message": "An error occurred (UnprocessableEntityException) when calling the
 GetSensitiveDataOccurrences operation: OBJECT_UNAVAILABLE"
}
```

Dans l'exemple précédent, Macie a tenté de récupérer des échantillons de l'objet S3 concerné, mais celui-ci n'est plus disponible. Le contenu de l'objet a changé après que Macie a créé la découverte.

Si votre demande aboutit mais qu'un autre type d'erreur a empêché Macie de récupérer et de révéler des échantillons de données sensibles pour la recherche, vous recevez un résultat similaire à ce qui suit :

```
{
    "error": "Macie can't retrieve the samples. You're not allowed to access the
 affected S3 object or the object is encrypted with a key that you're not allowed to
 use.",
    "status": "ERROR"
}
```

La valeur du `status` champ est `ERROR` et le `error` champ décrit l'erreur survenue. Les informations de la rubrique précédente peuvent vous aider à étudier l'erreur.

Schéma JSON pour les emplacements de données sensibles

Amazon Macie utilise des structures JSON standardisées pour stocker des informations sur l'emplacement des données sensibles dans les objets Amazon Simple Storage Service (Amazon S3). Les structures sont utilisées pour les découvertes de données sensibles et les résultats de

découverte de données sensibles. Pour les résultats de recherche de données sensibles, les structures font partie du schéma JSON pour les résultats. Pour consulter le schéma JSON complet à la recherche de résultats, consultez la section Résultats dans la référence des API Amazon Macie. Pour en savoir plus sur les résultats de la découverte de données sensibles, consultezStockage et conservation des résultats de découverte de données sensibles.

Rubriques

Présentation du schéma JSON pour les emplacements de données sensibles

Pour signaler l'emplacement des données sensibles qu'Amazon Macie a trouvées dans un objet S3 concerné, le schéma JSON pour les découvertes de données sensibles et les résultats de découverte de données sensibles inclut un `customDataIdentifiers` objet et un `sensitiveData` objet. L'`customDataIdentifiers`objet fournit des détails sur les données que Macie a détectées à l'aide d'identifiants de données personnalisés. L'`sensitiveData`objet fournit des détails sur les données que Macie a détectées à l'aide d'identifiants de données gérés.

Chaque `sensitiveData` objet `customDataIdentifiers` et contient un ou plusieurs `detections` tableaux :

- Dans un `customDataIdentifiers` objet, le `detections` tableau indique quels identifiants de données personnalisés ont détecté les données et ont produit la découverte. Pour chaque identifiant de données personnalisé, le tableau indique également le nombre d'occurrences des données détectées par l'identifiant. Il peut également indiquer l'emplacement des données détectées par l'identifiant.
- Dans un `sensitiveData` objet, un `detections` tableau indique les types de données sensibles que Macie a détectés à l'aide d'identifiants de données gérés. Pour chaque type de données sensibles, le tableau indique également le nombre d'occurrences des données et peut indiquer l'emplacement des données.

Pour la recherche de données sensibles, un `detections` tableau peut inclure 1 à 15 `occurrences` objets. Chaque `occurrences` objet indique où Macie a détecté des occurrences individuelles d'un type spécifique de données sensibles.

Par exemple, le `detections` tableau suivant indique l'emplacement de trois occurrences de données sensibles (numéros de sécurité sociale américains) que Macie a trouvées dans un fichier CSV.


```
"sensitiveData": [
     {
       "category": "PERSONAL_INFORMATION",
       "detections": [
          {
             "count": 30,
             "occurrences": {
                "cells": [
                   {
                      "cellReference": null,
                      "column": 1,
                      "columnName": "SSN",
                      "row": 2
                   },
                   {
                      "cellReference": null,
                      "column": 1,
                      "columnName": "SSN",
                      "row": 3
                   },
                   {
                      "cellReference": null,
                      "column": 1,
                      "columnName": "SSN",
                      "row": 4
                   }
                ]
             },
             "type": "USA_SOCIAL_SECURITY_NUMBER"
          }
```


L'emplacement et le nombre d'`occurrences`objets d'un `detections` tableau varient en fonction des catégories, des types et du nombre d'occurrences de données sensibles détectées par Macie au cours d'un cycle d'analyse automatique de découverte de données sensibles ou de l'exécution d'une tâche de découverte de données sensibles. Pour chaque cycle d'analyse ou exécution de tâche, Macie utilise un algorithme de recherche en profondeur pour renseigner les résultats obtenus avec des données de localisation correspondant à 1 à 15 occurrences de données sensibles détectées

par Macie dans des objets S3. Ces occurrences indiquent les catégories et les types de données sensibles qu'un bucket et un objet S3 concernés peuvent contenir.

Un `occurrences` objet peut contenir l'une des structures suivantes, selon le type de fichier ou le format de stockage de l'objet S3 concerné :

- `cells`tableau — Ce tableau s'applique aux classeurs Microsoft Excel, aux fichiers CSV et aux fichiers TSV. Un objet de ce tableau indique une cellule ou un champ dans lequel Macie a détecté une occurrence de données sensibles.
- `lineRanges`tableau : ce tableau s'applique aux fichiers de messages électroniques (EML) et aux fichiers texte non binaires autres que les fichiers CSV, JSON, JSON Lines et TSV, par exemple les fichiers HTML, TXT et XML. Un objet de ce tableau indique une ligne ou une plage complète de lignes dans laquelle Macie a détecté la présence de données sensibles, ainsi que la position des données sur la ou les lignes spécifiées.

  Dans certains cas, un objet d'une `lineRanges` matrice indique l'emplacement d'une détection de données sensibles dans un type de fichier ou un format de stockage pris en charge par un autre type de matrice. Ces cas sont les suivants : une détection dans une section non structurée d'un fichier autrement structuré, tel qu'un commentaire dans un fichier ; une détection dans un fichier mal formé que Macie analyse comme du texte brut ; et un fichier CSV ou TSV contenant un ou plusieurs noms de colonne dans lesquels Macie a détecté des données sensibles.
- `offsetRanges`array — Ce tableau est réservé pour une utilisation future. Si ce tableau est présent, sa valeur est nulle.
- `pages`tableau : ce tableau s'applique aux fichiers Adobe Portable Document Format (PDF). Un objet de ce tableau indique une page dans laquelle Macie a détecté une occurrence de données sensibles.
- `records`array — Ce tableau s'applique aux conteneurs d'objets Apache Avro, aux fichiers Apache Parquet, aux fichiers JSON et aux fichiers JSON Lines. Pour les conteneurs d'objets Avro et les fichiers Parquet, un objet de ce tableau indique un index d'enregistrement et le chemin d'accès à un champ d'un enregistrement dans lequel Macie a détecté la présence de données sensibles. Pour les fichiers JSON et JSON Lines, un objet de ce tableau indique le chemin d'accès à un champ ou à un tableau dans lequel Macie a détecté une occurrence de données sensibles. Pour les fichiers JSON Lines, il indique également l'index de la ligne qui contient les données.

Le contenu de ces tableaux varie en fonction du type de fichier ou du format de stockage de l'objet S3 concerné et de son contenu.

Détails et exemples du schéma JSON pour les emplacements de données sensibles

Amazon Macie adapte le contenu des structures JSON qu'il utilise pour indiquer où il a détecté des données sensibles dans des types de fichiers et de contenus spécifiques. Les rubriques suivantes expliquent et fournissent des exemples de ces structures.

Rubriques

Pour obtenir la liste complète des structures JSON pouvant être incluses dans une recherche de données sensibles, consultez la section Résultats de la référence des API Amazon Macie.

Réseau de cellules

S'applique aux classeurs Microsoft Excel, aux fichiers CSV et aux fichiers TSV

Dans un `cells` tableau, un `Cell` objet indique une cellule ou un champ dans lequel Macie a détecté une occurrence de données sensibles. Le tableau suivant décrit l'objectif de chaque champ d'un `Cell` objet.

Champ	Type	Description
`cellReference`	Chaîne	Emplacement de la cellule, en tant que référence absolue de cellule, qui contient l'occurrence. Ce champ s'applique uniquement aux classeurs Excel. Cette valeur est nulle pour les fichiers CSV et TSV.
`column`	Entier	Le numéro de colonne de la colonne qui contient l'occurrence. Pour un classeur Excel, cette valeur est en corrélation avec le ou les caractères

Champ	Type	Description
		alphabétiques d'un identifiant de colonne, par exemple, pour la colonne A, 1 pour la colonne B, 2 etc.
`columnName`	Chaîne	Le nom de la colonne qui contient l'occurrence, s'il est disponible.
`row`	Entier	Le numéro de ligne de la ligne qui contient l'occurrence.

L'exemple suivant montre la structure d'un `Cell` objet qui indique l'emplacement d'une occurrence de données sensibles détectées par Macie dans un fichier CSV.

```
"cells": [
   {
      "cellReference": null,
      "column": 3,
      "columnName": "SSN",
      "row": 5
   }
]
```

Dans l'exemple précédent, le résultat indique que Macie a détecté des données sensibles dans le champ de la cinquième ligne de la troisième colonne (nommée SSN) du fichier.

L'exemple suivant montre la structure d'un `Cell` objet qui indique l'emplacement d'une occurrence de données sensibles détectée par Macie dans un classeur Excel.

```
"cells": [
   {
      "cellReference": "Sheet2!C5",
      "column": 3,
      "columnName": "SSN",
      "row": 5
   }
]
```

Dans l'exemple précédent, le résultat indique que Macie a détecté des données sensibles dans la feuille de calcul nommée Sheet2 dans le classeur. Dans cette feuille de travail, Macie a détecté des données sensibles dans la cellule de la cinquième ligne de la troisième colonne (colonne C, nommée SSN).

LineRangesréseau

S'applique aux fichiers de messages électroniques (EML) et aux fichiers texte non binaires autres que les fichiers CSV, JSON, JSON Lines et TSV, par exemple les fichiers HTML, TXT et XML

Dans un `lineRanges` tableau, un `Range` objet indique une ligne ou une plage complète de lignes dans laquelle Macie a détecté la présence de données sensibles, ainsi que la position des données sur la ou les lignes spécifiées.

Cet objet est souvent vide pour les types de fichiers pris en charge par d'autres types de tableaux dans les `occurrences` objets. Les exceptions sont les suivantes :

- Données figurant dans des sections non structurées d'un fichier autrement structuré, telles qu'un commentaire dans un fichier.
- Données d'un fichier mal formé que Macie analyse en tant que texte brut.
- Un fichier CSV ou TSV contenant un ou plusieurs noms de colonne dans lesquels Macie a détecté des données sensibles.

Le tableau suivant décrit l'objectif de chaque champ d'un `Range` objet d'un `lineRanges` tableau.

Champ	Type	Description
`end`	Entier	Le nombre de lignes entre le début du fichier et la fin de l'occurrence.
`start`	Entier	Le nombre de lignes entre le début du fichier et le début de l'occurrence.
`startColumn`	Entier	Le nombre de caractère s, espaces compris et commençant par 1, entre

Champ	Type	Description
		le début de la première ligne contenant l'occurrence (`start`) et le début de l'occurrence.

L'exemple suivant montre la structure d'un `Range` objet qui indique l'emplacement d'une occurrence de données sensibles détectées par Macie sur une seule ligne d'un fichier TXT.

```
"lineRanges": [
   {
      "end": 1,
      "start": 1,
      "startColumn": 119
   }
]
```

Dans l'exemple précédent, le résultat indique que Macie a détecté une occurrence complète de données sensibles (une adresse postale) dans la première ligne du fichier. Le premier caractère de l'occurrence est composé de 119 caractères (espaces compris) à partir du début de cette ligne.

L'exemple suivant montre la structure d'un `Range` objet qui indique l'emplacement d'une occurrence de données sensibles qui s'étend sur plusieurs lignes dans un fichier TXT.

```
"lineRanges": [
   {
      "end": 54,
      "start": 51,
      "startColumn": 1
   }
]
```

Dans l'exemple précédent, le résultat indique que Macie a détecté une occurrence de données sensibles (une adresse postale) sur les lignes 51 à 54 du fichier. Le premier caractère de l'occurrence est le premier caractère de la ligne 51 du fichier.

Tableau de pages

S'applique aux fichiers Adobe Portable Document Format (PDF)

Dans un `pages` tableau, un `Page` objet indique une page dans laquelle Macie a détecté une occurrence de données sensibles. L'objet contient un `pageNumber` champ. Le `pageNumber` champ stocke un entier qui indique le numéro de page de la page qui contient l'occurrence.

L'exemple suivant montre la structure d'un `Page` objet qui indique l'emplacement d'une occurrence de données sensibles détectée par Macie dans un fichier PDF.

```
"pages": [
   {
      "pageNumber": 10
   }
]
```

Dans l'exemple précédent, le résultat indique que la page 10 du fichier contient l'occurrence.

Tableau d'enregistrements

S'applique aux conteneurs d'objets Apache Avro, aux fichiers Apache Parquet, aux fichiers JSON et aux fichiers JSON Lines

Pour un conteneur d'objets Avro ou un fichier Parquet, un `Record` objet dans un `records` tableau indique un index d'enregistrement et le chemin d'accès à un champ d'un enregistrement dans lequel Macie a détecté une occurrence de données sensibles. Pour les fichiers JSON et JSON Lines, un `Record` objet indique le chemin d'accès à un champ ou à un tableau dans lequel Macie a détecté une occurrence de données sensibles. Pour les fichiers JSON Lines, il indique également l'index de la ligne qui contient l'occurrence.

Le tableau suivant décrit l'objectif de chaque champ d'un `Record` objet.

Champ	Type	Description
`jsonPath`	Chaîne	Le chemin, sous forme d'expression JSONPath, menant à l'occurrence. Pour un conteneur d'objets Avro ou un fichier Parquet, il s'agit du chemin vers le champ de l'enregistrement

Champ	Type	Description
		(`recordIndex`) qui contient l'occurrence. Pour un fichier JSON ou JSON Lines, il s'agit du chemin d'accès au champ ou au tableau qui contient l'occurrence. Si les données sont une valeur d'un tableau, le chemin indique également quelle valeur contient l'occurrence. Si Macie détecte des données sensibles dans le nom d'un élément du chemin, Macie omet le `jsonPath` champ d'un objet. `Record` Si le nom d'un élément de chemin dépasse 240 caractères, Macie le tronque en supprimant les caractères du début du nom. Si le chemin complet obtenu dépasse 250 caractères, Macie tronque également le chemin, en commençant par le premier élément du chemin, jusqu'à ce que le chemin contienne 250 caractères ou moins.

Champ	Type	Description
`recordIndex`	Entier	Pour un conteneur d'objets Avro ou un fichier Parquet, l'index de l'enregistrement, en commençant par 0, pour l'enregistrement qui contient l'occurrence. Pour un fichier JSON Lines, l'index de ligne, commençant par 0, de la ligne qui contient l'occurrence. Cette valeur concerne toujours `0` les fichiers JSON.

L'exemple suivant montre la structure d'un `Record` objet qui indique l'emplacement d'une occurrence de données sensibles détectée par Macie dans un fichier Parquet.

```
"records": [
   {
      "jsonPath": "$['abcdefghijklmnopqrstuvwxyz']",
      "recordIndex": 7663
   }
]
```

Dans l'exemple précédent, le résultat indique que Macie a détecté des données sensibles dans l'enregistrement d'index 7663 (numéro d'enregistrement 7664). Dans cet enregistrement, Macie a détecté des données sensibles dans le champ nomméabcdefghijklmnopqrstuvwxyz. Le chemin JSON complet vers le champ de l'enregistrement est`$.abcdefghijklmnopqrstuvwxyz`. Le champ est un descendant direct de l'objet racine (niveau externe).

L'exemple suivant montre également la structure d'un `Record` objet en cas d'occurrence de données sensibles détectée par Macie dans un fichier Parquet. Toutefois, dans cet exemple, Macie a tronqué le nom du champ qui contient l'occurrence parce que le nom dépasse la limite de caractères.

```
"records": [
   {
      "jsonPath":
 "$['...uvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyzabc
```

```
      "recordIndex": 7663
   }
]
```

Dans l'exemple précédent, le champ est un descendant direct de l'objet racine (niveau externe).

Dans l'exemple suivant, également pour une occurrence de données sensibles détectée par Macie dans un fichier Parquet, Macie a tronqué le chemin complet du champ contenant l'occurrence. Le chemin complet dépasse la limite de caractères.

```
"records": [
   {
      "jsonPath":
 "$..usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.usssn10.usssn11.usssn12.usssn13.us
      "recordIndex": 2335
   }
]
```

Dans l'exemple précédent, le résultat indique que Macie a détecté des données sensibles dans l'enregistrement d'index 2335 (numéro d'enregistrement 2336). Dans cet enregistrement, Macie a détecté des données sensibles dans le champ nomméabcdefghijklmnopqrstuvwxyz. Le chemin JSON complet vers le champ de l'enregistrement est le suivant :

```
$['1234567890']usssn1.usssn2.usssn3.usssn4.usssn5.usssn6.usssn7.usssn8.usssn9.us
```

L'exemple suivant montre la structure d'un `Record` objet qui indique l'emplacement d'une occurrence de données sensibles détectée par Macie dans un fichier JSON. Dans cet exemple, l'occurrence est une valeur spécifique dans un tableau.

```
"records": [
   {
      "jsonPath": "$.access.key[2]",
      "recordIndex": 0
   }
]
```

Dans l'exemple précédent, le résultat indique que Macie a détecté des données sensibles dans la deuxième valeur d'un tableau nommékey. Le tableau est un enfant d'un objet nomméaccess.

L'exemple suivant montre la structure d'un `Record` objet qui spécifie l'emplacement d'une occurrence de données sensibles détectée par Macie dans un fichier JSON Lines.

```
"records": [
   {
      "jsonPath": "$.access.key",
      "recordIndex": 3
   }
]
```

Dans l'exemple précédent, le résultat indique que Macie a détecté des données sensibles dans la troisième valeur (ligne) du fichier. Sur cette ligne, l'occurrence se trouve dans un champ nommé`key`, qui est un enfant d'un objet nommé`access`.

Supprimer les résultats d'Amazon Macie

Pour rationaliser votre analyse des résultats, vous pouvez créer et utiliser des règles de suppression. Une règle de suppression est un ensemble de critères de filtrage basés sur des attributs qui définissent les cas dans lesquels vous souhaitez qu'Amazon Macie archive automatiquement les résultats. Les règles de suppression sont utiles lorsque vous avez examiné une catégorie de résultats et que vous ne souhaitez pas en être informé à nouveau.

Par exemple, vous pouvez décider d'autoriser les compartiments S3 à contenir des adresses postales s'ils n'autorisent pas l'accès public et qu'ils chiffrent automatiquement les nouveaux objets avec une adresse particulière. AWS KMS key Dans ce cas, vous pouvez créer une règle de suppression qui spécifie des critères de filtrage pour les champs suivants : type de détection des données sensibles, autorisation d'accès public au compartiment S3 et identifiant de clé KMS de chiffrement du compartiment S3. La règle supprime les résultats futurs qui correspondent aux critères du filtre.

Si vous supprimez les résultats à l'aide d'une règle de suppression, Macie continue de générer des résultats pour les occurrences ultérieures de données sensibles et les violations potentielles des politiques qui répondent aux critères de la règle. Cependant, Macie change automatiquement le statut des résultats en « archivé ». Cela signifie que les résultats n'apparaissent pas par défaut sur la console Amazon Macie, mais qu'ils y sont conservés jusqu'à leur expiration. Macie conserve les résultats pendant 90 jours.

En outre, Macie ne publie pas les résultats supprimés sur Amazon EventBridge sous forme d'événements ou pourAWS Security Hub. Macie continue toutefois à créer et à stocker des résultats de découverte de données sensibles en corrélation avec les résultats de découverte de données sensibles que vous supprimez. Cela permet de garantir que vous disposez d'un historique immuable

des résultats relatifs aux données sensibles dans le cadre des audits ou des enquêtes que vous effectuez en matière de confidentialité et de protection des données.

> **Note**
>
> Si votre compte fait partie d'une organisation qui gère de manière centralisée plusieurs comptes Macie, les règles de suppression peuvent fonctionner différemment pour votre compte. Cela dépend de la catégorie de résultats que vous souhaitez supprimer et du fait que vous possédez un compte administrateur ou membre Macie :
>
> - Conclusions relatives aux politiques — Seul un administrateur Macie peut supprimer les conclusions relatives aux politiques relatives aux comptes de l'organisation.
>
>   Si vous avez un compte administrateur Macie et que vous créez une règle de suppression, Macie applique la règle aux conclusions des politiques relatives à tous les comptes de votre organisation, sauf si vous configurez la règle pour exclure des comptes spécifiques. Si vous avez un compte de membre Macie et que vous souhaitez supprimer les informations relatives aux politiques relatives à votre compte, contactez votre administrateur Macie.
> - Découverte de données sensibles : un administrateur Macie et des membres individuels peuvent supprimer les découvertes de données sensibles produites par leurs tâches de découverte de données sensibles. Un administrateur Macie peut également supprimer les résultats générés par Macie lors de la découverte automatique de données sensibles pour l'organisation.
>
>   Seul le compte qui crée une tâche de découverte de données sensibles peut supprimer ou accéder aux découvertes de données sensibles produites par la tâche. Seul le compte administrateur Macie d'une organisation peut supprimer ou accéder aux résultats produits par la découverte automatique de données sensibles pour les comptes de l'organisation.
>
> Pour plus d'informations sur les tâches que les administrateurs et les membres peuvent effectuer, consultezComprendre la relation entre les comptes d'administrateur et de membre d'Amazon Macie.

Pour créer et gérer des règles de suppression, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie. Les rubriques suivantes expliquent comment procéder. Pour l'API, les rubriques incluent des exemples de la manière d'effectuer ces tâches à l'aide de AWS Command

Line Interface(AWS CLI). Vous pouvez également effectuer ces tâches en utilisant la version actuelle d'un autre outil de ligne de AWS commande ou d'un AWS SDK, ou en envoyant des requêtes HTTPS directement à Macie. Pour plus d'informations sur AWS les outils et les SDK, consultez la section Outils sur AWS lesquels vous pouvez vous appuyer.

Rubriques

Création de règles de suppression

Avant de créer une règle de suppression, il est important de noter que vous ne pouvez pas restaurer (désarchiver) les résultats que vous avez supprimés à l'aide d'une règle de suppression. Vous pouvez toutefois consulter les résultats supprimés sur la console Amazon Macie et accéder aux résultats supprimés grâce à l'API Amazon Macie.

Lorsque vous créez une règle de suppression, vous spécifiez des critères de filtre, un nom et, éventuellement, une description de la règle. Vous pouvez créer une règle de suppression à l'aide de la console Amazon Macie ou de l'API Amazon Macie.

Console

Suivez ces étapes pour créer une règle de suppression à l'aide de la console Amazon Macie.

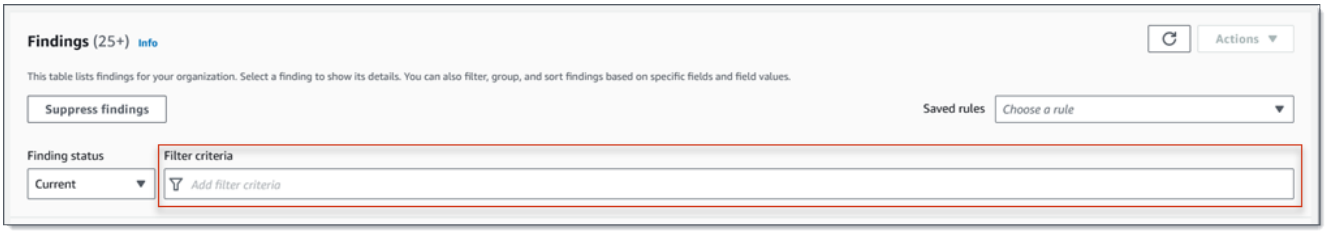
Pour créer une règle de suppression

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Conclusions.

> **Tip**
>
> Pour utiliser une règle de suppression ou de filtrage existante comme point de départ, choisissez-la dans la liste Règles enregistrées.
> Vous pouvez également rationaliser la création d'une règle en faisant d'abord pivoter et en analysant les résultats par un groupe logique prédéfini. Dans ce cas, Macie crée et applique automatiquement les conditions de filtre appropriées, ce qui peut

constituer un point de départ utile pour créer une règle. Pour ce faire, choisissez Par compartiment, Par type ou Par tâche dans le volet de navigation (sous Résultats), puis choisissez un élément dans le tableau. Dans le panneau de détails, choisissez le lien vers lequel le champ doit être pivoté.

3. Dans la zone Critères de filtre, ajoutez des conditions de filtre qui spécifient les attributs des résultats que vous souhaitez que la règle supprime.



Pour savoir comment ajouter des conditions de filtre, voirCréation et application de filtres aux résultats.

4. Lorsque vous avez fini d'ajouter des conditions de filtre pour la règle, choisissez Supprimer les résultats.
5. Sous Règle de suppression, entrez un nom et, éventuellement, une description de la règle.
6. Choisissez Save (Enregistrer).

API

Pour créer une règle de suppression par programmation, utilisez le CreateFindingsFilterfonctionnement de l'API Amazon Macie et spécifiez les valeurs appropriées pour les paramètres requis :

- Pour le `action` paramètre, spécifiez `ARCHIVE` pour vous assurer que Macie supprime les résultats correspondant aux critères de la règle.
- Pour le `criterion` paramètre, spécifiez une carte des conditions qui définissent les critères de filtre pour la règle.

  Dans la carte, chaque condition doit spécifier un champ, un opérateur et une ou plusieurs valeurs pour le champ. Le type et le nombre de valeurs dépendent du champ et de l'opérateur que vous choisissez. Pour plus d'informations sur les champs, les opérateurs et les types de valeurs que vous pouvez utiliser dans une condition Champs pour filtrer les résultatsUtilisation d'opérateurs dans des conditions, reportez-vous aux sections etSpécification de valeurs pour les champs.

Pour créer une règle de suppression à l'aide deAWS CLI, exécutez la create-findings-filtercommande et spécifiez les valeurs appropriées pour les paramètres requis. Les exemples suivants créent une règle de suppression qui renvoie toutes les données sensibles trouvées dans la version actuelle Région AWS et signalent les occurrences d'adresses postales (et aucun autre type de données sensibles) dans les objets S3.

Cet exemple est formaté pour Linux, macOS ou Unix et utilise le caractère de continuation de ligne inversée (\) pour améliorer la lisibilité.

```
$ aws macie2 create-findings-filter \
--action ARCHIVE \
--name my_suppression_rule \
--finding-criteria '{"criterion":
{"classificationDetails.result.sensitiveData.detections.type":{"eqExactMatch":
["ADDRESS"]}}}'
```

Cet exemple est formaté pour Microsoft Windows et utilise le caractère de continuation de ligne caret (^) pour améliorer la lisibilité.

```
C:\> aws macie2 create-findings-filter ^
--action ARCHIVE ^
--name my_suppression_rule ^
--finding-criteria={\"criterion\":
{\"classificationDetails.result.sensitiveData.detections.type\":{\"eqExactMatch\":
[\"ADDRESS\"]}}}
```

Où :

- *my_suppression_rule est le nom personnalisé de la règle*.
- criterionest une carte des conditions de filtrage pour la règle :
  - *ClassificationDetails.Result.SensitiveData.Detections.type est le nom JSON du champ Type de détection de* données sensibles.
  - *eqExactMatch*spécifie l'opérateur de correspondance exacte égal à égal.
  - *ADDRESS* est une valeur énumérée pour le champ Type de détection de données sensibles.

Si la commande s'exécute correctement, vous recevez une sortie similaire à ce qui suit.

```
{
```

```
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-
aa2f-4940-b347-d1451example",
    "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

Où se `arn` trouve le nom de ressource Amazon (ARN) de la règle de suppression créée et `id` l'identifiant unique de la règle.

Pour d'autres exemples de critères de filtre, voirFiltrer les résultats par programmation à l'aide de l'API Amazon Macie.

Révision des résultats supprimés

Par défaut, Macie n'affiche pas les résultats supprimés sur la console Amazon Macie. Toutefois, vous pouvez consulter ces résultats sur la console en modifiant les paramètres de votre filtre.

Pour consulter les résultats supprimés sur la console

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Conclusions. La page Résultats affiche les résultats que Macie a créés ou mis à jour pour votre compte au Région AWS cours des 90 derniers jours. Par défaut, cela n'inclut pas les résultats supprimés par une règle de suppression.
3. Pour Rechercher le statut, effectuez l'une des opérations suivantes :
   - Pour afficher uniquement les résultats supprimés, choisissez Archivé.
   - Pour afficher à la fois les résultats supprimés et non supprimés, sélectionnez Tout.
   - Pour masquer à nouveau les résultats supprimés, choisissez Current.

Vous pouvez également accéder aux résultats supprimés à l'aide de l'API Amazon Macie. Pour récupérer la liste des résultats supprimés, utilisez l'ListFindingsopération et incluez une condition `true` de filtre spécifique au `archived` champ. Pour un exemple de la procédure à suivre à l'aide duAWS CLI, voirFiltrer les résultats de manière programmatique. Pour récupérer ensuite les détails d'un ou de plusieurs résultats supprimés, utilisez l'GetFindingsopération et spécifiez l'identifiant unique pour chaque résultat à récupérer.

Modification des règles de suppression

Vous pouvez modifier les paramètres d'une règle de suppression à tout moment à l'aide de la console Amazon Macie ou de l'API Amazon Macie. Vous pouvez également attribuer et gérer des balises pour la règle.

Un tag est un label que vous définissez et attribuez à certains types de AWS ressources. Chaque balise comprend une clé de balise obligatoire et une valeur de balise facultative. Les balises peuvent vous aider à identifier, à classer et à gérer les ressources de différentes manières, par exemple en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Pour en savoir plus, consultez Marquage des ressources Amazon Macie.

Console

Suivez ces étapes pour modifier les paramètres d'une règle de suppression existante à l'aide de la console Amazon Macie.

Pour modifier une règle de suppression

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Conclusions.
3. Dans la liste des règles enregistrées, cliquez sur l'icône de modification () à côté de la règle de suppression que vous souhaitez modifier.
4. Effectuez l'une des actions suivantes :

   - Pour modifier les critères de la règle, utilisez la zone Critères de filtre pour saisir les conditions qui spécifient les attributs des résultats que vous souhaitez que la règle supprime. Pour savoir comment procéder, veuillez consulter la section Création et application de filtres aux résultats.
   - Pour modifier le nom de la règle, entrez un nouveau nom dans le champ Nom sous Règle de suppression.
   - Pour modifier la description de la règle, entrez une nouvelle description dans la zone Description sous Règle de suppression.
   - Pour attribuer, vérifier ou modifier des balises pour la règle, choisissez Gérer les balises sous Règle de suppression. Passez ensuite en revue et modifiez les balises si nécessaire. Une règle peut comporter jusqu'à 50 balises.

5. Une fois les modifications terminées, choisissez Save (Enregistrer).

API

Pour modifier une règle de suppression par programmation, utilisez l'UpdateFindingsFilterAPI Amazon Macie. Lorsque vous soumettez votre demande, utilisez les paramètres pris en charge pour spécifier une nouvelle valeur pour chaque paramètre que vous souhaitez modifier.

Pour le `id` paramètre, spécifiez l'identifiant unique de la règle à modifier. Vous pouvez obtenir cet identifiant en utilisant l'ListFindingsFilteropération pour récupérer une liste des règles de suppression et de filtrage pour votre compte. Si vous utilisez leAWS CLI, exécutez la list-findings-filterscommande pour récupérer cette liste.

Pour modifier une règle de suppression à l'aide deAWS CLI, exécutez la update-findings-filtercommande et utilisez les paramètres pris en charge pour spécifier une nouvelle valeur pour chaque paramètre que vous souhaitez modifier. Par exemple, la commande suivante modifie le nom d'une règle de suppression existante.

```
C:\> aws macie2 update-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example --
name mailing_addresses_only
```

Où :

- *8a3c5608-aa2f-4940-b347-d1451example* est l'identifiant unique de la règle.
- *mailing_addresses_only* est le nouveau nom de la règle.

Si la commande s'exécute correctement, vous recevez une sortie similaire à ce qui suit.

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a3c5608-
aa2f-4940-b347-d1451example",
    "id": "8a3c5608-aa2f-4940-b347-d1451example"
}
```

Où se `arn` trouve le nom de ressource Amazon (ARN) de la règle modifiée et `id` l'identifiant unique de la règle.

De même, l'exemple suivant convertit une règle de filtre en règle de suppression en modifiant la valeur du `action` paramètre de `NOOP` à`ARCHIVE`.

```
C:\> aws macie2 update-findings-filter --id 8a1c3508-aa2f-4940-b347-d1451example --
action ARCHIVE
```

Où :

- *8a1c3508-aa2f-4940-b347-d1451example* est l'identifiant unique de la règle.
- *ARCHIVE* est la nouvelle action que Macie doit exécuter sur les résultats qui répondent aux critères de la règle : supprimer les résultats.

Si la commande s'exécute correctement, vous recevez un résultat similaire à ce qui suit :

```
{
    "arn": "arn:aws:macie2:us-west-2:123456789012:findings-filter/8a1c3508-
aa2f-4940-b347-d1451example",
    "id": "8a1c3508-aa2f-4940-b347-d1451example"
}
```

Où se `arn` trouve le nom de ressource Amazon (ARN) de la règle modifiée et `id` l'identifiant unique de la règle.

Suppression de règles de suppression

Vous pouvez supprimer une règle de suppression à tout moment à l'aide de la console Amazon Macie ou de l'API Amazon Macie. Si vous supprimez une règle de suppression, Macie arrête de supprimer les occurrences nouvelles et ultérieures de résultats qui répondent aux critères de la règle et ne sont pas supprimés par d'autres règles. Notez toutefois que Macie peut continuer à supprimer les résultats qu'il est en train de traiter et à répondre aux critères de la règle.

Une fois que vous avez supprimé une règle de suppression, les occurrences nouvelles et suivantes de résultats correspondant aux critères de la règle ont le statut actuel (non archivé). Cela signifie qu'ils apparaissent par défaut sur la console Amazon Macie. En outre, Macie publie ces résultats sur Amazon EventBridge sous forme d'événements. En fonction des paramètres de publication de votre compte, Macie publie également les résultats sur. AWS Security Hub

Console

Procédez comme suit pour supprimer une règle de suppression à l'aide de la console Amazon Macie.

Pour supprimer une règle de suppression

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le volet de navigation, choisissez Conclusions.
3. Dans la liste des règles enregistrées, cliquez sur l'icône de modification (✎) à côté de la règle de suppression que vous souhaitez supprimer.
4. Sous Règle de suppression, choisissez Supprimer.

API

Pour supprimer une règle de suppression par programmation, utilisez l'DeleteFindingsFilterAPI Amazon Macie. Pour le `id` paramètre, spécifiez l'identifiant unique de la règle de suppression à supprimer. Vous pouvez obtenir cet identifiant en utilisant l'ListFindingsFilteropération pour récupérer une liste des règles de suppression et de filtrage pour votre compte. Si vous utilisez leAWS CLI, exécutez la list-findings-filterscommande pour récupérer cette liste.

Pour supprimer une règle de suppression à l'aide deAWS CLI, exécutez la delete-findings-filtercommande. Par exemple :

```
C:\> aws macie2 delete-findings-filter --id 8a3c5608-aa2f-4940-b347-d1451example
```

Où *8a3c5608-aa2f-4940-b347-d1451example* est l'identifiant unique de la règle de suppression à supprimer.

Si la commande s'exécute correctement, Macie renvoie une réponse HTTP 200 vide. Sinon, Macie renvoie une réponse HTTP 4 xx ou 500 indiquant pourquoi l'opération a échoué.

Évaluation de la gravité des résultats d'Amazon Macie

Lorsqu'Amazon Macie génère une politique ou une constatation de données sensibles, il attribue automatiquement une gravité à la constatation. La gravité d'un résultat reflète les principales caractéristiques du résultat et peut vous aider à évaluer et à prioriser vos résultats. La gravité d'une constatation n'implique ni n'indique le caractère critique ou l'importance que pourrait avoir une ressource affectée pour votre organisation.

En ce qui concerne les politiques, la gravité dépend de la nature d'un problème potentiel lié à la sécurité ou à la confidentialité d'un bucket à usage général Amazon Simple Storage Service (Amazon S3). Pour les découvertes de données sensibles, la gravité est basée sur la nature et le nombre d'occurrences de données sensibles trouvées par Macie dans un objet S3.

Dans Macie, la gravité d'une constatation est représentée de deux manières.

Niveau de gravité

Il s'agit d'une représentation qualitative de la gravité. Les niveaux de gravité varient de Low, pour les moins graves, à High, pour les plus graves.

Les niveaux de gravité apparaissent directement sur la console Amazon Macie. Ils sont également disponibles sous forme de représentations JSON des résultats sur la console Macie, à partir de l'API Amazon Macie, et dans les résultats de découverte de données sensibles corrélés aux résultats de données sensibles. Les niveaux de gravité sont également inclus dans la recherche des événements publiés par Macie sur Amazon EventBridge et des résultats sur lesquels Macie publie. AWS Security Hub

Score de sévérité

Il s'agit d'une représentation numérique de la gravité. Les scores de gravité vont de 1 à 3 et correspondent directement aux niveaux de gravité :

Score de sévérité	Niveau de gravité
1	Faible
2	Medium
3	Élevée

Les scores de gravité n'apparaissent pas directement sur la console Amazon Macie. Cependant, ils sont disponibles sous forme de représentations JSON des résultats sur la console Macie, à partir de l'API Amazon Macie, et dans les résultats de découverte de données sensibles corrélés aux résultats de données sensibles. Les scores de gravité sont également inclus dans la recherche d'événements publiés par Macie sur Amazon EventBridge. Ils ne sont pas inclus dans les résultats publiés par Macie. AWS Security Hub

Les rubriques de cette section indiquent comment Macie détermine la gravité des conclusions relatives aux politiques et des constatations relatives aux données sensibles.

Rubriques

Évaluation de la gravité des conclusions relatives aux politiques

La gravité d'une constatation de politique dépend de la nature d'un problème potentiel lié à la sécurité ou à la confidentialité d'un compartiment S3 à usage général. Le tableau suivant répertorie les niveaux de gravité que Macie attribue à chaque type de constatation de politique. Pour une description de chaque type, voirTypes de résultat.

Type de résultat	Niveau de gravité
Policy:IAMUser/S3BlockPublicAccessDisabled	Élevée
Policy:IAMUser/S3BucketEncryptionDisabled	Faible
Policy:IAMUser/S3BucketPublic	Élevée
Policy:IAMUser/S3BucketReplicatedExternally	Élevée
Policy:IAMUser/S3BucketSharedExternally	Élevée
Policy:IAMUser/S3BucketSharedWithCloudFront	Medium

La gravité d'une constatation de politique ne change pas en fonction du nombre d'occurrences de cette constatation.

Évaluation de la gravité des résultats relatifs aux données sensibles

La gravité d'une découverte de données sensibles dépend de la nature et du nombre d'occurrences de données sensibles trouvées par Macie dans un objet S3. Les rubriques suivantes indiquent comment Macie détermine la gravité de chaque type de détection de données sensibles :

- SensitiveData:S3Object/Credentials
- SensitiveData:S3Object/CustomIdentifier
- SensitiveData:S3Object/Financial
- SensitiveData:S3Object/Personal
- SensitiveData:S3Object/Multiple

Pour obtenir des informations détaillées sur les types de données sensibles que Macie peut détecter et signaler dans les résultats de données sensibles, consultez Utilisation des identificateurs de données gérés etCréation d'identificateurs de données personnalisés.

SensitiveData:S3Object/Credentials

R : La SensitiveDatarecherche de S3Object/Credentials indique qu'un objet S3 contient des données d'identification sensibles. Pour ce type de recherche, Macie détermine la gravité en fonction du type et du nombre d'occurrences des données d'identification trouvées par Macie dans l'objet.

Le tableau suivant indique les niveaux de gravité que Macie attribue aux résultats signalant des occurrences de données d'identification dans un objet S3.

Type de données sensibles	1 événement	2 à 99 occurrences	100 occurrences ou plus
AWS clé d'accès secrète	Élevée	Élevée	Élevée
Clé d'API Google Cloud	Élevée	Élevée	Élevée
En-tête d'autorisation HTTP Basic	Élevée	Élevée	Élevée
Jeton Web JSON (JWT)	Élevée	Élevée	Élevée
Clé privée OpenSSH	Élevée	Élevée	Élevée
Clé privée PGP	Élevée	Élevée	Élevée

Type de données sensibles	1 événement	2 à 99 occurrences	100 occurrences ou plus
Clé privée selon la norme de cryptographie à clé publique (PKCS)	Élevée	Élevée	Élevée
Clé privée PuTTY	Élevée	Élevée	Élevée
Clé d'API Stripe	Élevée	Élevée	Élevée

SensitiveData:S3Object/CustomIdentifier

A:S3Object/ SensitiveDatafinding CustomIdentifier indique qu'un objet S3 contient du texte qui correspond aux critères de détection d'un ou de plusieurs identifiants de données personnalisés. L'objet peut contenir plusieurs types de données sensibles.

Par défaut, Macie attribue le niveau de gravité moyen à ce type de découverte. Si l'objet S3 contient au moins une occurrence de texte correspondant aux critères de détection d'au moins un identifiant de données personnalisé, Macie attribue automatiquement le niveau de gravité moyen à la constatation. La gravité du résultat ne change pas en fonction du nombre d'occurrences de texte correspondant aux critères d'un identifiant de données personnalisé.

Toutefois, la gravité de ce type de constatation peut varier si vous avez défini des paramètres de gravité personnalisés pour un identifiant de données personnalisé à l'origine de la constatation. Si tel est le cas, Macie détermine la gravité comme suit :

- Si l'objet S3 contient du texte qui correspond aux critères de détection d'un seul identifiant de données personnalisé, Macie détermine la gravité du résultat en fonction des paramètres de gravité de cet identifiant.
- Si l'objet S3 contient du texte qui correspond aux critères de détection de plusieurs identificateurs de données personnalisés, Macie détermine la gravité du résultat en évaluant les paramètres de gravité pour chaque identifiant de données personnalisé, en déterminant lequel de ces paramètres produit le niveau de gravité le plus élevé, puis en attribuant le niveau de gravité le plus élevé au résultat.

Pour consulter les paramètres de gravité d'un identifiant de données personnalisé, choisissez Identifiants de données personnalisés dans le volet de navigation de la console Amazon Macie. Choisissez ensuite le nom de l'identifiant de données personnalisé. La section Sévérité présente les paramètres. Pour plus d'informations, consultez Définition des paramètres de gravité de la recherche pour les identificateurs de données personnalisés.

SensitiveData:S3Object/Financial

R : La SensitiveDataconstatation S3Object/Financial indique qu'un objet S3 contient des informations financières sensibles. Pour ce type de constatation, Macie détermine la gravité en fonction du type et du nombre d'occurrences des informations financières qu'elle a trouvées dans l'objet.

Le tableau suivant indique les niveaux de gravité que Macie attribue aux résultats signalant des occurrences d'informations financières dans un objet S3.

Type de données sensibles	1 événement	2 à 99 occurrences	100 occurrences ou plus
Compte bancaire numéro [1]	Élevée	Élevée	Élevée
Date d'expiration de carte de crédit	Faible	Medium	Élevée
Données relatives à la bande magnétique des cartes de crédit	Élevée	Élevée	Élevée
Numéro de carte de crédit [2]	Élevée	Élevée	Élevée
Code de vérification de carte de crédit	Medium	Élevée	Élevée

1. Les niveaux de gravité sont les mêmes pour tout type de numéro de compte bancaire, qu'il s'agisse d'un numéro de compte bancaire de base (BBAN), d'un numéro de compte bancaire international (IBAN) ou d'un numéro de compte bancaire canadien ou américain.
2. Les niveaux de gravité sont les mêmes pour les numéros de carte de crédit situés ou non à proximité d'un mot clé.

Si une constatation fait état de plusieurs types d'informations financières dans un objet, Macie détermine la gravité de la constatation en calculant la gravité de chaque type d'information financière trouvée par Macie, en déterminant quel type produit la gravité la plus élevée et en attribuant la gravité la plus élevée à la constatation. Par exemple, si Macie détecte 10 dates d'expiration de carte de crédit (niveau de gravité moyen) et 10 numéros de carte de crédit (niveau de gravité élevé) dans un objet, Macie attribue un niveau de gravité élevé au résultat.

SensitiveData:S3Object/Personal

R:S3Object/Personal SensitiveDatafinding indique qu'un objet S3 contient des informations personnelles sensibles : informations médicales personnelles (PHI), informations personnelles identifiables (PII) ou une combinaison des deux. Pour ce type de découverte, Macie détermine la gravité en fonction du type et du nombre d'occurrences des informations personnelles qu'elle a trouvées dans l'objet.

Le tableau suivant indique les niveaux de gravité que Macie attribue aux résultats de données sensibles signalant des occurrences de PHI dans un objet S3.

Type de données sensibles	1 événement	2 à 99 occurrences	100 occurrences ou plus
Numéro d'enregistrement de la Drug Enforcement Agency (DEA)	Élevée	Élevée	Élevée
Numéro de réclamation d'assurance maladie (HICN)	Élevée	Élevée	Élevée

Type de données sensibles	1 événement	2 à 99 occurrences	100 occurrences ou plus
Numéro d'assurance maladie ou d'identification médicale	Élevée	Élevée	Élevée
Code du système de codage des procédures communes pour les soins de santé (HCPCS)	Élevée	Élevée	Élevée
Code national des médicaments (NDC)	Élevée	Élevée	Élevée
Identifiant national du fournisseur (NPI)	Élevée	Élevée	Élevée
Identifiant unique de l'appareil (UDI)	Faible	Medium	Élevée

Le tableau suivant indique les niveaux de gravité que Macie attribue aux découvertes de données sensibles signalant des occurrences de PII dans un objet S3.

Type de données sensibles	1 événement	2 à 99 occurrences	100 occurrences ou plus
Date de naissance	Faible	Medium	Élevée
Numéro d'identification du permis de conduire	Faible	Medium	Élevée
Numéro de liste électorale	Élevée	Élevée	Élevée

Type de données sensibles	1 événement	2 à 99 occurrences	100 occurrences ou plus
Nom complet	Faible	Medium	Élevée
Coordonnées du système de positionnement global (GPS)	Faible	Medium	Medium
Cookie HTTP	Faible	Medium	Élevée
Adresse postale	Faible	Medium	Élevée
Numéro d'identification nationale	Élevée	Élevée	Élevée
Numéro d'assurance nationale (NINO)	Élevée	Élevée	Élevée
Numéro de passeport	Medium	Élevée	Élevée
Numéro de résidence permanente	Élevée	Élevée	Élevée
Phone number (Numéro de téléphone)	Faible	Medium	Élevée
Numéro d'assurance sociale (SIN)	Élevée	Élevée	Élevée
Numéro de sécurité sociale (SSN)	Élevée	Élevée	Élevée
Numéro d'identification ou de référence du contribuable	Élevée	Élevée	Élevée

Type de données sensibles	1 événement	2 à 99 occurrences	100 occurrences ou plus
Numéro d'identif ication du véhicule (VIN)	Faible	Faible	Medium

Si une découverte fait état de plusieurs types de PHI, de PII, ou à la fois de PHI et de PII dans un objet, Macie détermine la gravité du résultat en calculant la gravité de chaque type, en déterminant quel type produit la gravité la plus élevée et en attribuant cette gravité la plus élevée au résultat.

Par exemple, si Macie détecte 10 noms complets (niveau de gravité moyen) et 5 numéros de passeport (niveau de gravité élevé) dans un objet, Macie attribue un niveau de gravité élevé au résultat. De même, si Macie détecte 10 noms complets (niveau de gravité moyen) et 10 numéros d'identification d'assurance maladie (niveau de gravité élevé) dans un objet, Macie attribue un niveau de gravité élevé au résultat.

SensitiveData:S3Object/Multiple

R : La SensitiveDatarecherche S3Object/Multiple indique qu'un objet S3 contient des données appartenant à plusieurs catégories de données sensibles, c'est-à-dire toute combinaison de données d'identification, d'informations financières, d'informations personnelles ou de texte correspondant aux critères de détection d'un ou de plusieurs identifiants de données personnalisés.

Pour ce type de constatation, Macie détermine la gravité en calculant la gravité de chaque type de données sensibles qu'elle a trouvées (comme indiqué dans les rubriques précédentes), en déterminant quel type produit la gravité la plus élevée et en attribuant la gravité la plus élevée au résultat.

Par exemple, si Macie détecte 10 noms complets (niveau de gravité moyen) et 10 clés d'accès AWS secrètes (niveau de gravité élevé) dans un objet, Macie attribue un niveau de gravité élevé à la découverte.

Amazon Macie

Pour faciliter l'intégration avec d'autres applications, services et systèmes, tels que les systèmes de surveillance ou de gestion des événements, Amazon Macie publie automatiquement les résultats relatifs aux politiques et aux données sensibles sur Amazon EventBridge sous forme d'événements. Pour bénéficier d'une assistance supplémentaire et d'une analyse plus approfondie du niveau de sécurité de votre entreprise, vous pouvez configurer Macie pour qu'il publie également les résultats relatifs aux politiques et aux données sensibles sur. AWS Security Hub

Amazon EventBridge

AmazonEventBridge, anciennement Amazon CloudWatch Events, est un service de bus d'événements sans serveur qui fournit un flux de données en temps réel à partir d'applications et de services, puis achemine ces données vers des cibles telles que des AWS Lambda fonctions, les rubriques Amazon Vous pouvez ainsi automatiser la surveillance et le traitement de certains types d'événements, y compris les événements que Macie publie à des fins de résultats. EventBridge Pour en savoir plusEventBridge, consultez le guide de EventBridge l'utilisateur Amazon.

Si vous intégrez AWS User Notifications à Macie, vous pouvez également utiliser EventBridge des événements pour générer automatiquement des notifications concernant les événements que Macie publie pour obtenir des résultats. Les notifications utilisateur vous permettent de créer des règles personnalisées et de configurer des canaux de diffusion pour recevoir des notifications concernant des EventBridge événements qui vous intéressent. Les canaux de diffusion incluent les e-mails, les notifications par AWS Chatbot chat et les notifications AWS Console Mobile Application push. Vous pouvez également consulter les notifications de manière centralisée sur leAWS Management Console. Pour en savoir plus sur les notifications utilisateur, consultez le guide de l'utilisateur d'AWS User Notifications.

AWS Security Hub

AWS Security Hubest un service de sécurité qui fournit une vue complète de votre état de AWS sécurité. Il collecte des données de sécurité à partir Services AWS des solutions de type logiciel et vous permet de vérifier votre environnement par rapport aux normes et aux bonnes pratiques. AWS Partner Network Il vous permet également d'analyser les tendances en matière de tendances en matière de tendances et d'identifier les problèmes de la plus haute importance. Avec Security Hub, vous pouvez consulter les résultats de l'examen des résultats de l'analyse plus large de la posture de sécurité. Vous pouvez également agréger les résultats de plusieurs

Régions AWS, ainsi que surveiller et traiter les données de résultats agrégées provenant d'une seule région. Pour en savoir plus sur Security Hub, consultez le Guide de AWS Security Hub l'utilisateur.

Lorsque Macie crée une constatation, elle la publie automatiquement EventBridge sous la forme d'un nouvel événement. Selon les paramètres de publication que vous choisissez pour votre compte, Macie peut également publier les résultats sur Security Hub. Macie publie chaque nouvelle découverte immédiatement après la fin du traitement de la découverte. Si Macie détecte une occurrence ultérieure d'une constatation de politique existante, elle publie une mise à jour de l'EventBridgeévénement existant correspondant à cette constatation. Selon vos paramètres de publication, Macie peut également publier la mise à jour sur Security Hub. Macie publie ces mises à jour de manière récurrente, selon une fréquence de publication que vous spécifiez dans les paramètres de publication de votre compte.

Rubriques

Configuration des paramètres de publication pour les résultats d'Amazon Macie

Pour faciliter l'intégration avec d'autres applications, services et systèmes, Amazon Macie publie automatiquement les conclusions relatives aux politiques et aux données sensibles sur Amazon EventBridge sous forme d'événements. Pour plus d'informations sur la manière dont vous pouvez l'utiliser EventBridge pour surveiller et traiter les résultats, consultezIntégration d'Amazon Macie à Amazon EventBridge.

Vous pouvez AWS Security Hub également configurer Macie pour qu'il publie automatiquement les résultats, en utilisant les options de destination que vous spécifiez dans les paramètres de publication de votre compte. Grâce à ces options, vous pouvez configurer Macie pour publier uniquement les conclusions relatives aux politiques, uniquement les conclusions relatives aux données sensibles, ou à la fois les conclusions relatives aux politiques et aux données sensibles sur Security Hub. Vous

pouvez également configurer Macie pour arrêter de publier les résultats sur Security Hub. Pour plus d'informations sur la manière dont vous pouvez utiliser Security Hub pour surveiller et traiter les résultats, consultezIntégration d'Amazon Macie avec AWS Security Hub.

En ce qui concerne les conclusions relatives aux politiques, le moment auquel Macie publie une constatation à un autre Service AWS dépend du fait qu'il s'agit ou non de nouvelles conclusions et de la fréquence de publication que vous spécifiez pour votre compte. Pour les découvertes de données sensibles, le moment est toujours immédiat : Macie publie une découverte de données sensibles immédiatement après avoir fini de traiter la découverte. Contrairement aux conclusions relatives aux politiques, Macie traite toutes les découvertes relatives aux données sensibles comme nouvelles (uniques).

Notez que Macie ne publie pas de politiques ou de résultats de données sensibles qui sont archivés automatiquement par une règle de suppression. En d'autres termes, Macie ne publie pas les résultats supprimés à d'autres Services AWS.

Rubriques

Choix des destinations de publication pour les résultats

Vous pouvez configurer Amazon Macie pour publier automatiquement les politiques et les résultats relatifs aux données sensibles, AWS Security Hub en plus d'Amazon. EventBridge Par défaut, Macie publie uniquement les nouvelles conclusions et les mises à jour relatives aux politiques sur Security Hub. Pour modifier ou étendre la configuration par défaut, ajustez les paramètres de destination de publication pour votre compte.

Lorsque vous ajustez vos paramètres de destination, vous choisissez les catégories de conclusions que vous souhaitez que Macie publie sur Security Hub : uniquement les conclusions relatives aux politiques, uniquement les conclusions relatives aux données sensibles, ou à la fois les conclusions relatives aux politiques et aux données sensibles. Vous pouvez également choisir d'arrêter de publier toute catégorie de recherche dans Security Hub.

Si vous modifiez vos paramètres de destination, vos modifications s'appliquent uniquement aux paramètres actuels Région AWS. Si vous êtes l'administrateur Macie d'une organisation, votre

modification s'applique uniquement à votre compte. Elle ne s'applique à aucun compte de membre associé. Pour de plus amples informations, veuillez consulter Gestion de plusieurs comptes .

Pour choisir les destinations de publication des résultats

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Dans la section Publication des résultats, sous Destinations, choisissez l'une des options suivantes :

   - Publier les résultats des politiques sur Security Hub : cochez cette case pour commencer à publier automatiquement les résultats des politiques nouvelles et mises à jour sur Security Hub. Pour arrêter de publier des résultats de politique nouveaux et actualisés sur Security Hub, décochez cette case.

     Si vous cochez cette case et que vous avez des conclusions relatives aux politiques existantes, Macie ne les publie pas automatiquement sur Security Hub. Macie publie plutôt uniquement les résultats des politiques qu'il crée ou met à jour une fois que vous avez enregistré votre modification.
   - Publier les résultats de données sensibles sur Security Hub : cochez cette case pour commencer à publier automatiquement les nouveaux résultats de données sensibles sur Security Hub. Pour arrêter de publier les nouvelles découvertes relatives aux données sensibles sur Security Hub, décochez cette case.

     Si vous cochez cette case et que vous avez trouvé des données sensibles, Macie ne les publie pas automatiquement sur Security Hub. Au lieu de cela, Macie publie uniquement les résultats de données sensibles qu'il crée une fois que vous avez enregistré votre modification.
4. Choisissez Enregistrer.

Si vous avez choisi de publier une catégorie de résultats sur Security Hub, assurez-vous d'activer également Security Hub dans la région actuelle et de le configurer pour accepter les résultats de Macie. Dans le cas contraire, vous ne pourrez pas accéder aux résultats dans Security Hub. Pour savoir comment accepter les résultats dans Security Hub, consultez la section Gestion des intégrations de produits dans le guide de l'AWS Security Hub utilisateur.

Détermination de la fréquence de publication des résultats

Dans Amazon Macie, chaque résultat possède un identifiant unique. Macie utilise cet identifiant pour déterminer quand publier une découverte auprès d'un autre Service AWSutilisateur :

- Nouvelles découvertes — Lorsque Macie crée une nouvelle politique ou une nouvelle recherche de données sensibles, elle attribue un identifiant unique à la découverte dans le cadre du traitement de la découverte. Dès que Macie a fini de traiter le résultat, il le publie en tant que nouvel EventBridge événement Amazon. En fonction des paramètres de publication de votre compte, Macie publie également le résultat en tant que nouveau résultat dans AWS Security Hub.
- Conclusions mises à jour — Lorsque Macie détecte une occurrence ultérieure d'une constatation de politique existante, il met à jour la constatation existante en ajoutant des détails sur l'occurrence suivante et en augmentant le nombre d'occurrences. Macie publie également ces mises à jour de l' EventBridgeévénement existant et, en fonction des paramètres de publication de votre compte, de la découverte existante du Security Hub. Macie le fait uniquement pour les conclusions relatives aux politiques. Contrairement aux conclusions relatives aux politiques, les découvertes relatives aux données sensibles sont toutes traitées comme nouvelles (uniques).

  Par défaut, Macie publie des résultats mis à jour toutes les 15 minutes dans le cadre d'un cycle de publication récurrent. Cela signifie que toutes les conclusions relatives aux politiques mises à jour après le cycle de publication le plus récent seront conservées, mises à jour à nouveau si nécessaire et incluses dans le cycle de publication suivant (environ 15 minutes plus tard). Vous pouvez modifier cette planification en choisissant une fréquence de publication différente. Par exemple, si vous configurez Macie pour publier des résultats mis à jour toutes les heures et qu'une publication a lieu à 12h00, toutes les mises à jour effectuées après 12h00 sont publiées à 13h00.

Notez qu'aucun de ces cas ne s'applique aux résultats archivés automatiquement par une règle de suppression. Macie ne publie pas les résultats supprimés à d'autres Services AWS.

Modification de la fréquence de publication des résultats

Vous pouvez modifier le calendrier utilisé par Amazon Macie pour publier des mises à jour des conclusions relatives aux politiques existantes dans d'autres pays. Services AWSPar défaut, Macie publie des résultats mis à jour toutes les 15 minutes. Si vous modifiez cet horaire, votre modification s'applique uniquement au calendrier actuel Région AWS. Si vous êtes l'administrateur Macie d'une organisation, votre modification s'applique également à tous les comptes membres associés dans la région. Pour de plus amples informations, veuillez consulter Gestion de plusieurs comptes .

Pour modifier la fréquence de publication des résultats mis à jour

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Dans la section Publication des résultats, sous Fréquence de mise à jour des conclusions relatives aux politiques, choisissez la fréquence à laquelle vous souhaitez que Macie publie les résultats des politiques mises à jour à d'autres Services AWS.
4. Choisissez Enregistrer.

Intégration d'Amazon Macie à Amazon EventBridge

AmazonEventBridge, anciennement Amazon CloudWatch Events, est un service de bus événementiel sans serveur. EventBridgefournit un flux de données en temps réel à partir d'applications et de services, puis achemine ces données vers des cibles telles que des AWS Lambda fonctions, des rubriques Amazon Simple Notification Service (Amazon SNS) et des flux Amazon Kinesis. Pour en savoir plusEventBridge, consultez le guide de EventBridge l'utilisateur Amazon.

AvecEventBridge, vous pouvez automatiser la surveillance et le traitement de certains types d'événements. Cela inclut les événements qu'Amazon Macie publie automatiquement pour les nouvelles découvertes en matière de politiques et les découvertes de données sensibles. Cela inclut également les événements que Macie publie automatiquement pour les occurrences ultérieures de conclusions relatives aux politiques existantes. Pour savoir comment et quand Macie publie ces événements, consultezConfiguration des paramètres de publication pour les résultats.

En utilisant EventBridge les événements publiés par Macie pour les résultats, vous pouvez suivre et traiter les résultats en temps quasi réel. Vous pouvez ensuite agir en fonction des résultats en utilisant d'autres applications et services. Par exemple, vous pouvez utiliser EventBridge pour envoyer des types spécifiques de nouveaux résultats à une fonction AWS Lambda. La fonction Lambda peut ensuite traiter et envoyer les données à votre système de gestion des incidents et des événements de sécurité (SIEM). Si vous intégrez AWS User Notifications à Macie, vous pouvez également utiliser les événements pour être automatiquement informé des résultats via les canaux de diffusion que vous spécifiez.

Outre la surveillance et le traitement automatisés, l'utilisation de EventBridge permet de conserver à long terme les données de vos résultats. Macie conserve les résultats pendant 90 jours.

AvecEventBridge, vous pouvez envoyer les données de recherche vers votre plateforme de stockage préférée et stocker les données aussi longtemps que vous le souhaitez.

> **Note**
>
> Pour une conservation à long terme, configurez également Macie Un résultat de découverte de données sensibles est un enregistrement qui consigne les détails de l'analyse que Macie Pour en savoir plus, consultez Stockage et conservation des résultats de découverte de données sensibles.

Rubriques

Collaboration avec Amazon EventBridge

Avec AmazonEventBridge, vous créez des règles pour spécifier les événements que vous souhaitez surveiller et les cibles sur lesquelles vous souhaitez effectuer des actions automatisées pour ces événements. Une cible est une destination vers laquelle EventBridge des événements sont envoyés.

Pour automatiser les tâches de surveillance et de traitement des résultats, vous pouvez créer une EventBridge règle qui détecte automatiquement les événements de recherche d'Amazon Macie et envoie ces événements à une autre application ou à un autre service pour traitement ou autre action. Vous pouvez personnaliser la règle afin d'envoyer uniquement les événements qui répondent à certains critères. Pour ce faire, spécifiez des critères qui dérivent duEventBridge schéma d'événements pour les résultats.

Par exemple, vous pouvez créer une règle qui envoie des types de nouveau résultat spécifiques à une fonction AWS Lambda. La fonction Lambda peut ensuite effectuer des tâches telles que : traiter et envoyer les données à votre système SIEM ; appliquer automatiquement un certain type de chiffrement côté serveur à un objet S3 ; ou restreindre l'accès à un objet S3 en modifiant la liste de contrôle d'accès (ACL) de l'objet. Vous pouvez également créer une règle qui envoie automatiquement les nouveaux résultats de niveau de gravité élevé à une rubrique Amazon SNS, qui en informe ensuite votre équipe de réponse aux incidents.

Outre l'appel aux fonctions Lambda et l'envoi de notifications aux rubriques Amazon SNS, il prend en EventBridge charge d'autres types de cibles et d'actions, telles que le relais d'événements vers

des flux Amazon Kinesis Streams, l'activation de machines d'état et l'appel de la fonctionnalité Run Command d'autres types de cibles et d'actions, telles que le relais d'événements vers des flux Amazon Kinesis Streams, AWS Step Functions l'activation de machines d'état et l'appel AWS Systems Manager Pour plus d'informations sur les cibles prises en charge, consultez EventBridgeles cibles Amazon dans le Guide de EventBridge l'utilisateur Amazon.

Création de EventBridge règles Amazon pour les résultats

Les procédures suivantes expliquent comment utiliser la EventBridge console Amazon et le AWS Command Line Interface(AWS CLI) pour créer une EventBridge règle pour les résultats d'Amazon Macie. La règle détecte les EventBridge événements qui utilisent le schéma et le modèle d'événement des résultats Macie, puis envoyer ces événements à une AWS Lambda fonction pour l'exécution.

AWS Lambda est un service de calcul qui permet d'exécuter du code sans avoir à mettre en service ni à gérer des serveurs. Vous empaquetez votre code et le téléchargez dans AWS Lambda en tant que fonction Lambda. AWS Lambda exécute alors la fonction lorsque la fonction est appelée. Une fonction peut être appelée manuellement, par vous, automatiquement en réponse à des événements, ou en réponse à des demandes d'applications ou de services. Pour plus d'informations sur la création et l'appel de fonctions Lambda, consultez le Guide du AWS Lambda développeur.

Console

Cette procédure explique comment utiliser la EventBridge console Amazon pour créer une règle qui envoie automatiquement tous les événements de recherche Macie à une fonction Lambda pour traitement. La règle utilise les paramètres par défaut pour les règles qui s'exécutent lorsque des événements spécifiques sont reçus. Pour en savoir plus sur les paramètres des règles ou pour savoir comment créer une règle utilisant des paramètres personnalisés, consultez la section Création de règles qui réagissent aux événements dans le Guide de EventBridge l'utilisateur Amazon.

> **Tip**
>
> Vous pouvez également créer une règle qui utilise un modèle personnalisé pour détecter un sous-ensemble d'événements de recherche Macie Ce sous-ensemble peut être basé sur des champs spécifiques que Macie Pour de plus amples informations sur les champs disponibles, veuillez consulter EventBridge schéma d'événements pour les résultats. Pour

savoir comment créer ce type de règle, consultez la section Filtrage du contenu dans les modèles d'événements du Guide de EventBridge l'utilisateur Amazon.

Avant de créer cette règle, créez la fonction Lambda que la règle doit utiliser comme cible. Lorsque vous créez la règle, vous devez spécifier cette fonction comme étant la cible de la règle.

Pour créer une règle d'événement à l'aide de la console

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Sous Events (Événements) dans le panneau de navigation, choisissez Rules (Règles).
3. Dans la section Rules (Règles) choisissez Create rule (Créer une règle).
4. Sur la page Définir les détails de la règle, procédez comme suit :
   - Pour Name (Nom), entrez le nom de la règle.
   - (Facultatif) Dans le champ Description, saisissez une brève description de la règle.
   - Pour le bus d'événements, assurez-vous que la valeur par défaut est sélectionnée et que l'option Activer la règle sur le bus d'événements sélectionné est activée.
   - Pour Rule type (Type de règle), choisissez Rule with an event pattern (Règle avec un modèle d'événement).
5. Lorsque vous avez terminé, choisissez Suivant.
6. Sur la page Créer un modèle d'événement, procédez comme suit :
   - Pour Event Source, choisissez AWSEvents ou EventBridge Partner.
   - (Facultatif) Pour Exemple d'événement, consultez un exemple d'événement de recherche pour Macie afin de savoir ce qu'un événement peut contenir. Pour ce faire, choisissez AWSdes événements. Ensuite, pour Exemples d'événements, choisissez Macie Finding.
   - Pour Modèle d'événement, choisissez Formulaire de modèle d'événement. Définissez ensuite les paramètres suivants :
     - Pour Event source (Source d'événement), choisissez Services AWS.
     - Pour Service AWS, entrez Macie.
     - Dans Type d'événement, saisissez Macie Finding.
7. Lorsque vous avez terminé, choisissez Suivant.
8. Sur la page Sélectionner les cibles, procédez comme suit :

- Pour Target types (Types de cibles), choisissez Service AWS.
- Pour Sélectionner une cible, entrez la fonction Lambda. Ensuite, pour Function, choisissez la fonction Lambda à laquelle vous souhaitez envoyer des événements de recherche.
- Pour Configurer la version/l'alias, saisissez les paramètres de version et d'alias pour la fonction Lambda cible.
- (Facultatif) Pour les paramètres supplémentaires, entrez des paramètres personnalisés pour spécifier les données d'événement que vous souhaitez envoyer à la fonction Lambda. Vous pouvez également spécifier comment gérer les événements qui ne sont pas transmis correctement à la fonction.

9. Lorsque vous avez terminé, choisissez Suivant.
10. Sur la page Configurer les balises, saisissez éventuellement une ou plusieurs balises à affecter à la règle. Sélectionnez ensuite Next (Suivant).
11. Sur la page Vérifier et créer, passez en revue les paramètres de la règle et vérifiez qu'ils sont corrects.

    Pour modifier un paramètre, choisissez Modifier dans la section qui contient le paramètre, puis entrez le paramètre approprié. Vous pouvez également utiliser les onglets de navigation pour accéder à la page qui contient un paramètre.
12. Lorsque vous avez fini de vérifier les paramètres, choisissez Créer une règle.

AWS CLI

Cette procédure explique comment utiliser le AWS CLI pour créer une EventBridge règle qui envoie tous les événements de recherche Macie à une fonction Lambda pour traitement. La règle utilise les paramètres par défaut pour les règles qui s'exécutent lorsque des événements spécifiques sont reçus. Dans la procédure, les commandes sont formatées pour Microsoft Windows. Pour Linux, macOS ou Unix, remplacez le caractère de continuation de ligne du curseur (^) par une barre oblique inverse (\).

Avant de créer cette règle, créez la fonction Lambda que la règle doit utiliser comme cible. Lorsque vous créez la fonction, notez son ARN (Amazon Resource Name). Vous devrez entrer cet ARN lors de la spécification de la cible de la règle.

Pour créer une règle d'événement à l'aide de l'AWS CLI

1. Créez une règle qui détecte les événements associés à tous les résultats sur lesquels Macie publie. EventBridge Pour ce faire, utilisez la commande EventBridge put-rule. Par exemple :

```
C:\> aws events put-rule ^
--name MacieFindings ^
--event-pattern "{\"source\":[\"aws.macie\"]}"
```

Où se *MacieFindings*trouve le nom que vous souhaitez attribuer à la règle ?

Si la commande s'exécute correctement, EventBridge répond avec l'ARN de la règle. Notez cet ARN. Vous devrez l'entrer au cours de l'étape 3.

> **Tip**
>
> Vous pouvez également créer une règle qui utilise un modèle personnalisé pour détecter un sous-ensemble d'événements de recherche Macie Ce sous-ensemble peut être basé sur des champs spécifiques que Macie Pour de plus amples informations sur les champs disponibles, veuillez consulter EventBridge schéma d'événements pour les résultats. Pour savoir comment créer ce type de règle, consultez la section Filtrage du contenu dans les modèles d'événements du Guide de EventBridge l'utilisateur Amazon.

2. Spécifiez la fonction Lambda à utiliser comme cible pour la règle. Pour ce faire, utilisez la commande EventBridge put-targets. Par exemple :

```
C:\> aws events put-targets ^
--rule MacieFindings ^
--targets Id=1,Arn=arn:aws:lambda:regionalEndpoint:accountID:function:my-
findings-function
```

Où *MacieFindings*est le nom que vous avez spécifié pour la règle lors de l'étape 1, et la valeur du `Arn` paramètre est l'ARN de la fonction que vous souhaitez que la règle utilise comme cible.

3. Ajoutez des autorisations permettant à la règle d'appeler la fonction Lambda cible. Pour ce faire, utilisez la commande Lambda add-permission. Par exemple :

```
C:\> aws lambda add-permission ^
--function-name my-findings-function ^
--statement-id Sid ^
--action lambda:InvokeFunction ^
--principal events.amazonaws.com ^
--source-arn arn:aws:events:regionalEndpoint:accountId:rule:MacieFindings
```

Où :

- *my-findings-function*est le nom de la fonction Lambda que vous souhaitez que la règle utilise comme cible.
- *Sid* est un identifiant d'instruction que vous définissez pour décrire l'instruction dans la politique de la fonction Lambda.
- `source-arn` est l'ARN de la règle EventBridge.

Si la commande s'exécute correctement, vous obtenez un résultat similaire à ce qui suit :

```
{
  "Statement": "{\"Sid\":\"sid\",
    \"Effect\":\"Allow\",
    \"Principal\":{\"Service\":\"events.amazonaws.com\"},
    \"Action\":\"lambda:InvokeFunction\",
    \"Resource\":\"arn:aws:lambda:us-east-1:111122223333:function:my-findings-
function\",
    \"Condition\":
      {\"ArnLike\":
        {\"AWS:SourceArn\":
         \"arn:aws:events:us-east-1:111122223333:rule/MacieFindings\"}}}"
}
```

La valeur `Statement` est une version de la chaîne JSON correspondant à l'instruction ajoutée à la politique de la fonction Lambda.

Intégration d'Amazon Macie avec AWS Security Hub

AWS Security Hubest un service qui vous fournit une vue complète de votre niveau de sécurité dans l'ensemble de votre AWS environnement et vous aide à vérifier que votre environnement est

conforme aux normes et aux meilleures pratiques du secteur de la sécurité. Pour ce faire, il utilise, agrège, organise et hiérarchise les résultats issus de multiples solutions de AWS Partner Network sécurité prises Services AWS en charge. Security Hub vous aide à analyser les tendances en matière de sécurité et à identifier les problèmes de sécurité les plus prioritaires. Avec Security Hub, vous pouvez également agréger les résultats de plusieursRégions AWS, puis surveiller et traiter toutes les données de résultats agrégées provenant d'une seule région. Pour en savoir plus sur Security Hub, consultez le guide de AWS Security Hub l'utilisateur.

Amazon Macie s'intègre à Security Hub, ce qui signifie que vous pouvez publier automatiquement les résultats de Macie vers Security Hub. Security Hub peut ensuite inclure ces résultats dans son analyse de votre posture de sécurité. En outre, vous pouvez utiliser Security Hub pour surveiller et traiter les conclusions relatives aux politiques et aux données sensibles dans le cadre d'un ensemble plus vaste et agrégé de données de conclusions pour votre AWS environnement. En d'autres termes, vous pouvez analyser les résultats de Macie tout en effectuant des analyses plus larges de la posture de sécurité de votre entreprise, et corriger les résultats si nécessaire. Security Hub simplifie le traitement de volumes importants de résultats provenant de plusieurs fournisseurs. En outre, il utilise un format standard pour tous les résultats, y compris ceux de Macie. L'utilisation de ce format, le format ASFF (AWSSecurity Finding Format), vous évite d'avoir à effectuer des efforts de conversion de données fastidieux.

Rubriques

Comment Amazon Macie publie ses résultats sur AWS Security Hub

Dans AWS Security Hub, les problèmes de sécurité sont suivis en tant que résultats. Certains résultats proviennent de problèmes détectés par Amazon MacieServices AWS, par exemple, ou par des solutions de AWS Partner Network sécurité prises en charge. Security Hub utilise également un ensemble de règles pour détecter les problèmes de sécurité et générer des résultats.

Security Hub fournit des outils pour gérer les résultats provenant de toutes ces sources. Vous pouvez consulter et filtrer les listes de résultats et examiner les détails des résultats individuels. Pour savoir comment procéder, consultez la section Affichage des listes de recherche et des informations

détaillées dans le guide de AWS Security Hub l'utilisateur. Vous pouvez également suivre le statut d'une analyse dans un résultat. Pour savoir comment procéder, reportez-vous à la section Agir en fonction des résultats dans le Guide de AWS Security Hub l'utilisateur.

Tous les résultats dans Security Hub utilisent un format JSON standard appelé AWS Security Finding Format (ASFF). L'ASFF inclut des détails sur la source d'un problème, les ressources concernées et l'état actuel d'une découverte. Pour de plus amples informations, veuillez consulter AWS Security Finding Format (ASFF) dans le Guide de l'utilisateur AWS Security Hub.

Types de résultats publiés par Macie

Selon les paramètres de publication que vous choisissez pour votre compte Macie, Macie peut publier toutes les conclusions qu'il crée sur Security Hub, qu'il s'agisse de données sensibles ou de conclusions relatives aux politiques. Pour plus d'informations sur ces paramètres et sur la façon de les modifier, consultezConfiguration des paramètres de publication pour les résultats. Par défaut, Macie publie uniquement les nouvelles conclusions et les mises à jour relatives aux politiques sur Security Hub. Macie ne publie pas les résultats de données sensibles sur Security Hub.

Résultats de données sensibles

Si vous configurez Macie pour publier les résultats de données sensibles sur Security Hub, Macie publie automatiquement chaque recherche de données sensibles créée pour votre compte et il le fait immédiatement après avoir terminé de traiter le résultat. Macie le fait pour toutes les découvertes de données sensibles qui ne sont pas archivées automatiquement par une règle de suppression.

Si vous êtes l'administrateur Macie d'une organisation, la publication est limitée aux résultats des tâches de découverte de données sensibles que vous avez exécutées et aux activités automatisées de découverte de données sensibles effectuées par Macie pour votre organisation. Seul le compte qui crée une tâche peut publier les résultats des données sensibles produites par la tâche. Seul le compte administrateur Macie peut publier les résultats relatifs aux données sensibles produits par la découverte automatique de données sensibles pour son organisation.

Lorsque Macie publie des résultats de données sensibles sur Security Hub, il utilise le format ASFF (AWSSecurity Finding Format), qui est le format standard pour tous les résultats de Security Hub. Dans l'ASFF, le `Types` champ indique le type de résultat. Ce champ utilise une taxonomie légèrement différente de la taxonomie des types de recherche dans Macie.

Le tableau suivant répertorie le type de recherche ASFF pour chaque type de recherche de données sensibles que Macie peut créer.

Type de recherche Macie	Type de résultat ASFF
SensitiveData:S3Object/Credentials	Sensitive Data Identifications/Passwords/SensitiveData:S3Object-Credentials
SensitiveData:S3Object/CustomIdentifier	Sensitive Data Identifications/PII/SensitiveData:S3Object-CustomIdentifier
SensitiveData:S3Object/Financial	Sensitive Data Identifications/Financial/SensitiveData:S3Object-Financial
SensitiveData:S3Object/Multiple	Sensitive Data Identifications/PII/SensitiveData:S3Object-Multiple
SensitiveData:S3Object/Personal	Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal

Résultats de la stratégie

Si vous configurez Macie pour publier les résultats des politiques sur Security Hub, Macie publie automatiquement chaque nouvelle constatation de stratégie créée et il le fait immédiatement après avoir terminé de traiter les résultats. Si Macie détecte une occurrence ultérieure d'une constatation de politique existante, il publie automatiquement une mise à jour de cette constatation dans Security Hub, en utilisant une fréquence de publication que vous spécifiez pour votre compte. Macie exécute ces tâches pour toutes les conclusions relatives aux politiques qui ne sont pas archivées automatiquement par une règle de suppression.

Si vous êtes l'administrateur Macie d'une organisation, la publication se limite aux conclusions relatives aux politiques relatives aux compartiments S3 appartenant directement à votre compte. Macie ne publie pas les résultats des politiques qu'il crée ou met à jour pour les comptes des membres de votre organisation. Cela permet de s'assurer que vous n'avez pas de données de résultats dupliquées dans Security Hub.

Comme c'est le cas pour les découvertes relatives aux données sensibles, Macie utilise le format ASFF (AWSSecurity Finding Format) lorsqu'il publie des résultats politiques nouveaux et actualisés

sur Security Hub. Dans l'ASFF, le `Types` champ utilise une taxonomie légèrement différente de la taxonomie des types de recherche dans Macie.

Le tableau suivant répertorie le type de recherche ASFF pour chaque type de recherche de politique que Macie peut créer. Si Macie a créé ou mis à jour un résultat de politique dans Security Hub le 28 janvier 2021 ou après cette date, le résultat possède l'une des valeurs suivantes pour le `Types` champ ASFF dans Security Hub.

Type de recherche Macie	Type de résultat ASFF
Policy:IAMUser/S3BlockPublicAccessDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BlockPublicAccessDisabled
Policy:IAMUser/S3BucketEncryptionDisabled	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketEncryptionDisabled
Policy:IAMUser/S3BucketPublic	Effects/Data Exposure/Policy:IAMUser-S3BucketPublic
Policy:IAMUser/S3BucketReplicatedExternally	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketReplicatedExternally
Policy:IAMUser/S3BucketSharedExternally	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketSharedExternally
Policy:IAMUser/S3BucketSharedWithCloudFront	Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-S3BucketSharedWithCloudFront

Si Macie a créé ou mis à jour pour la dernière fois une constatation de politique avant le 28 janvier 2021, la recherche possède l'une des valeurs suivantes pour le `Types` champ ASFF dans Security Hub :

- Policy:IAMUser/S3BlockPublicAccessDisabled
- Policy:IAMUser/S3BucketEncryptionDisabled
- Policy:IAMUser/S3BucketPublic
- Policy:IAMUser/S3BucketReplicatedExternally
- Policy:IAMUser/S3BucketSharedExternally

Les valeurs de la liste précédente correspondent directement aux valeurs du champ Type de recherche (`type`) dans Macie.

> **Note**
>
> Lorsque vous examinez et traitez les conclusions relatives aux politiques dans Security Hub, notez les exceptions suivantes :
>
> - Dans certains casRégions AWS, Macie a commencé à utiliser les types de résultats ASFF pour des découvertes nouvelles et mises à jour dès le 25 janvier 2021.
> - Si vous avez donné suite à une constatation de politique dans Security Hub avant que Macie ne commence à utiliser les types de recherche ASFF dans votre rechercheRégion AWS, la valeur du `Types` champ ASFF de la recherche sera l'un des types de recherche Macie de la liste précédente. Il ne s'agira pas de l'un des types de recherche ASFF du tableau précédent. Cela est vrai pour les conclusions de politique auxquelles vous avez donné suite à l'aide de la AWS Security Hub console ou du BatchUpdateFindings fonctionnement de l'AWS Security HubAPI.

Latence pour la publication des résultats

Lorsque Macie crée une nouvelle politique ou une nouvelle recherche de données sensibles, il publie la découverte sur Security Hub immédiatement après avoir terminé de traiter la recherche.

Lorsque Macie détecte une occurrence ultérieure d'une constatation de politique existante, il publie une mise à jour de la constatation existante du Security Hub. Le moment de la mise à jour dépend de la fréquence de publication que vous choisissez pour votre compte Macie. Par défaut, Macie publie

des mises à jour toutes les 15 minutes. Pour plus d'informations, notamment pour savoir comment modifier les paramètres de votre compte, consultezConfiguration des paramètres de publication pour les résultats.

Nouvelle tentative de publication lorsque Security Hub n'est pas disponible

Si Security Hub n'est pas disponible, Macie crée une file de résultats qui n'ont pas été reçus par Security Hub. Lorsque le système est restauré, Macie tente à nouveau de publier jusqu'à ce que les résultats soient reçus par Security Hub.

Mise à jour des résultats existants dans Security Hub

Une fois que Macie a publié une constatation de politique sur Security Hub, Macie la met à jour pour refléter toute occurrence supplémentaire de l'activité de recherche ou de recherche. Macie le fait uniquement pour les conclusions relatives aux politiques. Contrairement aux conclusions relatives aux politiques, les découvertes relatives aux données sensibles sont toutes traitées comme nouvelles (uniques).

Lorsque Macie publie une mise à jour d'une constatation de politique, Macie met à jour la valeur du champ Updated At (`UpdatedAt`) de la constatation. Vous pouvez utiliser cette valeur pour déterminer à quel moment Macie a récemment détecté une occurrence ultérieure d'une violation potentielle de la politique ou du problème à l'origine de cette constatation.

Macie peut également mettre à jour la valeur du champ Types (`Types`) d'une recherche si la valeur existante du champ n'est pas un type de recherche ASFF. Cela dépend si vous avez donné suite à la constatation dans Security Hub. Si vous n'avez pas donné suite au résultat, Macie remplace la valeur du champ par le type de recherche ASFF approprié. Si vous avez donné suite au résultat, en utilisant la AWS Security Hub console ou en BatchUpdateFindings utilisant l'AWS Security Hub API, Macie ne modifie pas la valeur du champ.

Exemples de découvertes d'Amazon Macie dans AWS Security Hub

Lorsqu'Amazon Macie publie ses résultats surAWS Security Hub, il utilise le format ASFF (AWSSecurity Finding Format). Il s'agit du format standard pour tous les résultats de Security Hub. Les exemples suivants utilisent des exemples de données pour illustrer la structure et la nature des données de résultats que Macie publie sur Security Hub dans ce format :

- Exemple de découverte de données sensibles
- Exemple de constatation relative à une politique

Exemple de découverte de données sensibles dans Security Hub

Voici un exemple de découverte de données sensibles publiée par Macie sur Security Hub à l'aide de l'ASFF.


```
{
    "SchemaVersion": "2018-10-08",
    "Id": "5be50fce24526e670df77bc00example",
    "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/macie",
    "ProductName": "Macie",
    "CompanyName": "Amazon",
    "Region": "us-east-1",
    "GeneratorId": "aws/macie",
    "AwsAccountId": "111122223333",
    "Types":[
        "Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal"
    ],
    "CreatedAt": "2022-05-11T10:23:49.667Z",
    "UpdatedAt": "2022-05-11T10:23:49.667Z",
    "Severity": {
        "Label": "HIGH",
        "Normalized": 70
    },
    "Title": "The S3 object contains personal information.",
    "Description": "The object contains personal information such as first or last
 names, addresses, or identification numbers.",
    "ProductFields": {
        "JobArn": "arn:aws:macie2:us-east-1:111122223333:classification-
job/698e99c283a255bb2c992feceexample",
        "S3Object.Path": "DOC-EXAMPLE-BUCKET1/2022 Sourcing.tsv",
        "S3Object.Extension": "tsv",
        "S3Bucket.effectivePermission": "NOT_PUBLIC",
        "OriginType": "SENSITIVE_DATA_DISCOVERY_JOB",
        "S3Object.PublicAccess": "false",
        "S3Object.Size": "14",
        "S3Object.StorageClass": "STANDARD",
        "S3Bucket.allowsUnencryptedObjectUploads": "TRUE",
        "JobId": "698e99c283a255bb2c992feceexample",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
macie/5be50fce24526e670df77bc00example",
        "aws/securityhub/ProductName": "Macie",
        "aws/securityhub/CompanyName": "Amazon"
    },
```

```
    "Resources": [
        {
            "Type": "AwsS3Bucket",
            "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
            "Partition": "aws",
            "Region": "us-east-1",
            "Details": {
                "AwsS3Bucket": {
                    "OwnerId":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example",
                    "OwnerName": "johndoe",
                    "OwnerAccountId": "444455556666",
                    "CreatedAt": "2020-12-30T18:16:25.000Z",
                    "ServerSideEncryptionConfiguration": {
                        "Rules": [
                            {
                                "ApplyServerSideEncryptionByDefault": {
                                    "SSEAlgorithm": "aws:kms",
                                    "KMSMasterKeyID": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                                }
                            }
                        ]
                    },
                    "PublicAccessBlockConfiguration": {
                        "BlockPublicAcls": true,
                        "BlockPublicPolicy": true,
                        "IgnorePublicAcls": true,
                        "RestrictPublicBuckets": true
                    }
                }
            }
        },
        {
            "Type": "AwsS3Object",
            "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1/2022 Sourcing.tsv",
            "Partition": "aws",
            "Region": "us-east-1",
            "DataClassification": {
                "DetailedResultsLocation": "s3://macie-data-discovery-results/
AWSLogs/111122223333/Macie/us-east-1/
                698e99c283a255bb2c992feceexample/111122223333/32b8485d-4f3a-3aa1-be33-
aa3f0example.jsonl.gz",
                "Result":{
```

```
                    "MimeType": "text/tsv",
                    "SizeClassified": 14,
                    "AdditionalOccurrences": false,
                    "Status": {
                        "Code": "COMPLETE"
                    },
                    "SensitiveData": [
                        {
                            "Category": "PERSONAL_INFORMATION",
                            "Detections": [
                                {
                                    "Count": 1,
                                    "Type": "USA_SOCIAL_SECURITY_NUMBER",
                                    "Occurrences": {
                                        "Cells": [
                                            {
                                                "Column": 10,
                                                "Row": 1,
                                                "ColumnName": "Other"
                                            }
                                        ]
                                    }
                                }
                            ],
                            "TotalCount": 1
                        }
                    ],
                    "CustomDataIdentifiers": {
                        "Detections": [
                        ],
                        "TotalCount": 0
                    }
                }
            },
            "Details": {
                "AwsS3Object": {
                    "LastModified": "2022-04-22T18:16:46.000Z",
                    "ETag": "ebe1ca03ee8d006d457444445example",
                    "VersionId": "SlBC72z5hArgexOJifxw_IN57example",
                    "ServerSideEncryption": "aws:kms",
                    "SSEKMSKeyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                }
            }
```

```
        }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "HIGH"
        },
        "Types": [
            "Sensitive Data Identifications/PII/SensitiveData:S3Object-Personal"
        ]
    },
    "Sample": false,
    "ProcessedAt": "2022-05-11T10:23:49.667Z"
}
```

Exemple de découverte d'une politique dans Security Hub

Voici un exemple d'une nouvelle constatation de politique publiée par Macie sur Security Hub dans l'ASFF.

```
{
    "SchemaVersion": "2018-10-08",
    "Id": "36ca8ba0-caf1-4fee-875c-37760example",
    "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/macie",
    "ProductName": "Macie",
    "CompanyName": "Amazon",
    "Region": "us-east-1",
    "GeneratorId": "aws/macie",
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/AWS Security Best Practices/Policy:IAMUser-
S3BlockPublicAccessDisabled"
    ],
    "CreatedAt": "2022-04-24T09:27:43.313Z",
    "UpdatedAt": "2022-04-24T09:27:43.313Z",
    "Severity": {
        "Label": "HIGH",
        "Normalized": 70
    },
```

```
    "Title": "Block Public Access settings are disabled for the S3 bucket",
    "Description": "All Amazon S3 block public access settings are disabled for the
 Amazon S3 bucket. Access to the bucket is
      controlled only by access control lists (ACLs) or bucket policies.",
    "ProductFields": {
        "S3Bucket.effectivePermission": "NOT_PUBLIC",
        "S3Bucket.allowsUnencryptedObjectUploads": "FALSE",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
macie/36ca8ba0-caf1-4fee-875c-37760example",
        "aws/securityhub/ProductName": "Macie",
        "aws/securityhub/CompanyName": "Amazon"
    },
    "Resources": [
        {
        "Type": "AwsS3Bucket",
        "Id": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
        "Partition": "aws",
        "Region": "us-east-1",
        "Tags": {
            "Team": "Recruiting",
            "Division": "HR"
        },
        "Details": {
            "AwsS3Bucket": {
              "OwnerId":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example",
              "OwnerName": "johndoe",
              "OwnerAccountId": "444455556666",
              "CreatedAt": "2020-11-25T18:24:38.000Z",
              "ServerSideEncryptionConfiguration": {
                "Rules": [
                    {
                    "ApplyServerSideEncryptionByDefault": {
                        "SSEAlgorithm": "aws:kms",
                        "KMSMasterKeyID": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                    }
                  }
                ]
              },
              "PublicAccessBlockConfiguration": {
                "BlockPublicAcls": false,
                "BlockPublicPolicy": false,
                "IgnorePublicAcls": false,
```

```
                "RestrictPublicBuckets": false
               }
            }
         }
      }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "HIGH"
        },
        "Types": [
            "Software and Configuration Checks/AWS Security Best Practices/
Policy:IAMUser-S3BlockPublicAccessDisabled"
        ]
    },
    "Sample": false
}
```

Activation et configuration de AWS Security Hub l'intégration

Pour intégrer Amazon Macie àAWS Security Hub, activez Security Hub pour votre. Compte AWS Pour savoir comment procéder, consultez la section Enabling Security Hub dans le guide de AWS Security Hub l'utilisateur.

Lorsque vous activez Macie et Security Hub, l'intégration est automatiquement activée. Par défaut, Macie commence à publier automatiquement les résultats des politiques nouvelles et mises à jour sur Security Hub. Il n'est pas nécessaire de prendre des mesures supplémentaires pour configurer l'intégration. Si vous avez des conclusions relatives aux politiques existantes lorsque l'intégration est activée, Macie ne les publie pas sur Security Hub. Macie publie plutôt uniquement les résultats des politiques qu'il crée ou met à jour une fois l'intégration activée.

Vous pouvez éventuellement personnaliser votre configuration en choisissant la fréquence à laquelle Macie publie les mises à jour des résultats des politiques dans Security Hub. Vous pouvez également choisir de publier les résultats relatifs aux données sensibles sur Security Hub. Pour savoir comment procéder, veuillez consulter la section Configuration des paramètres de publication pour les résultats.

Arrêt de la publication des résultats à AWS Security Hub

Pour arrêter de publier les résultats surAWS Security Hub, vous pouvez modifier les paramètres de publication de votre compte Amazon Macie. Pour savoir comment procéder, veuillez consulter la section Choix des destinations de publication pour les résultats. Vous pouvez également le faire à l'aide de la console Security Hub ou de l'API Security Hub. Pour savoir comment procéder, consultez la section Désactivation et activation du flux de résultats d'une intégration (console) ou Désactivation du flux de résultats d'une intégration (API Security Hub, AWS CLI) dans le guide de l'AWS Security Hubutilisateur.

Intégration d'Amazon Macie à AWS User Notifications

AWS User Notifications est un service qui centralise vosAWS notifications sur leAWS Management Console. Cela inclut les notifications telles que les CloudWatch alarmes Amazon,AWS Support les cas et les communications provenant d'autres utilisateursServices AWS. Les notifications utilisateur vous permettent de configurer des règles et des canaux de diffusion personnalisés pour recevoir des notifications concernant certains types d' EventBridge événements Amazon. Les canaux de diffusion incluent les e-mails, les notifications parAWS Chatbot chat et les notificationsAWS Console Mobile Application push. Vous pouvez également consulter les notifications sur la console AWS User Notifications. Pour en savoir plus sur les notifications utilisateur, consultez le guide de l'utilisateur d'AWS User Notifications.

Macie s'intègre à AWS User Notifications, ce qui signifie que vous pouvez configurer les notifications utilisateur pour vous informer des événements sur lesquels Macie publie des informations sur EventBridge les politiques et les données sensibles. Si un événement de recherche correspond aux critères que vous spécifiez, User Notifications génère une notification. La notification inclut des informations clés sur le résultat associé, tels que le type et la gravité du résultat, ainsi que le nom de la ressource affectée. Les notifications utilisateur peuvent également envoyer la notification à un ou plusieurs canaux de distribution que vous spécifiez. Vous pouvez adapter votre choix de canaux de distribution en fonction de vos flux de travail en matière de sécurité et de conformité.

Par exemple, vous pouvez configurer les notifications utilisateur pour générer des notifications pour des types spécifiques de nouveaux résultats très graves. Vous pouvez également spécifierAWS Chatbot un canal de diffusion pour ces notifications. Les notifications utilisateur détectent ensuite les EventBridge événements liés aux résultats, génèrent des notifications qui incluent des données issues des résultats et envoient les notifications àAWS Chatbot. AWS Chatbotpeut ensuite acheminer les notifications vers un canal Slack ou un salon de discussion Amazon Chime pour informer votre équipe de réponse aux incidents.

Rubriques

Utilisation des AWS d'utilisateurs

Avec AWS User Notifications, vous créez des règles pour spécifier les types d' EventBridge événements Amazon que vous souhaitez surveiller et pour lesquels vous souhaitez recevoir des notifications. Une règle définit les critères auxquels un EventBridge événement doit répondre pour générer une notification. Vous pouvez également choisir un ou plusieurs canaux de diffusion pour une règle. Les canaux de diffusion indiquent où vous souhaitez recevoir des notifications pour les événements qui répondent aux critères d'une règle.

Si les notifications utilisateur détectent un EventBridge événement correspondant aux critères d'une règle, elles effectuent les tâches générales suivantes :

1. Extrait un sous-ensemble de données de l'événement.
2. Génère une notification qui contient les données extraites.
3. Envoie la notification aux canaux de diffusion que vous spécifiez pour ce type d'événement.

La conception et la structure de la notification sont optimisées pour chaque canal de diffusion auquel elle est envoyée.

Pour contrôler la fréquence ou le nombre de notifications que vous recevez, vous pouvez configurer les paramètres d'agrégation d'une règle. Si vous activez ces paramètres, les notifications utilisateur combinent les données de plusieurs événements en une seule notification. Vous pouvez choisir d'envoyer des notifications d'événements agrégées rapidement et fréquemment, ce que vous souhaiterez peut-être faire pour détecter des événements présentant un niveau de gravité élevé. Vous pouvez également les envoyer moins fréquemment pour recevoir moins de notifications, ce que vous pouvez faire pour les événements de recherche de faible gravité. Si vous combinez des données d'événements, vous pouvez effectuer une analyse détaillée pour consulter les détails de chaque événement agrégé à l'aide de la console AWS User Notifications. À partir de là, vous pouvez également accéder à chaque recherche associée sur la console Amazon Macie.

Activation et configuration des notifications utilisateur AWS pour les résultats d'Amazon Macie

Pour permettre à AWS User Notifications de générer des notifications concernant les résultats d'Amazon Macie, créez une configuration de notification pour Macie dans Notifications utilisateur. Une configuration de notification spécifie les critères d'une règle. Elle définit également les canaux de distribution et les autres paramètres permettant de surveiller et d'envoyer des notifications concernant les EventBridge événements Amazon qui répondent aux critères de la règle. Pour obtenir des informations détaillées sur la création d'une configuration de notification, consultez la section Prise en main d'AWS User Notifications dans le Guide de l'utilisateur d'AWS.

Pour créer une configuration de notification pour les résultats de Macie, choisissez les options suivantes pour la règle d'événement :

- Pour Service AWSIe nom, choisissez Macie.
- Pour Type d'événement, choisissez Macie Finding.
- Pour les régions, sélectionnezRégion AWS celles dans lesquelles vous utilisez Macie et souhaitez être informé des résultats.

Avec cette configuration, User Notifications surveille les EventBridge événements pour vousCompte AWS et génère des notifications pour tous les événements de recherche de Macie dans les régions que vous avez sélectionnées. Les événements répondent aux critères suivants :

- `source`est égal`aws.macie`
- `detail-type`est égal`Macie Finding`

Le modèle JSON sous-jacent de la règle d'événement est le suivant :

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"]
}
```

Pour affiner la règle et générer des notifications uniquement pour un sous-ensemble de résultats, vous pouvez personnaliser le modèle JSON de la règle. Pour ce faire, spécifiez des critères supplémentaires qui découlent du schéma desEventBridge événements pour les résultats de Macie.

Si vous créez une règle qui utilise un modèle JSON personnalisé, vous pouvez créer plusieurs configurations de notification pour les résultats de Macie. Vous pouvez ensuite personnaliser les canaux de diffusion et les autres paramètres pour chaque configuration afin de les aligner sur vos flux de travail de sécurité et de conformité pour des types de résultats spécifiques.

Par exemple, vous pouvez créer une règle qui vous avertit si Macie génère ou met à jour un Policy:IAMUser/S3BucketPublicrésultat. Dans ce cas, le modèle de la règle peut être le suivant :

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
        "type": ["Policy:IAMUser/S3BucketPublic"]
    }
}
```

Vous pouvez également créer une autre règle qui vous avertira si Macie génère une recherche de données sensibles pour un compartiment S3 accessible au public. Dans ce cas, le modèle de la règle peut être le suivant :

```
{
    "source": ["aws.macie"],
    "detail-type": ["Macie Finding"],
    "detail": {
        "type": [ { "prefix": "SensitiveData" } ],
        "resourcesAffected": {
            "effectivePermission": ["PUBLIC"]
        }
    }
}
```

Si vous créez plusieurs configurations de notification pour les résultats de Macie, il est conseillé de vous assurer que la règle pour chaque configuration est unique. Dans le cas contraire, vous risquez de recevoir des notifications dupliquées pour des résultats individuels.

Pour en savoir plus sur la personnalisation des modèles d'événements pour les règles, consultez la section Utilisation de modèles d'événements JSON personnalisés dans le guide de l'utilisateur d'AWS User Notifications.

Mappage des champs de notifications utilisateur AWS aux champs de recherche Amazon Macie

Lorsqu'AWS User Notifications génère une notification pour une découverte sur Amazon Macie, elle remplit la notification avec les données d'un sous-ensemble de champs de l' EventBridge événement Amazon correspondant. Ces champs fournissent des informations clés sur le résultat associé, tels que le type et la gravité du résultat, ainsi que le nom de la ressource affectée.

Si vous consultez une notification sur la console AWS User Notifications, la notification inclut toutes les données de ce sous-ensemble de champs. Il fournit également un lien vers la recherche associée sur la console Amazon Macie. Si vous consultez une notification dans d'autres canaux de diffusion, il se peut qu'elle ne contienne des données que pour certains champs. En effet, User Notifications adapte la conception et la structure de ses notifications pour qu'elles fonctionnent avec chaque type de canal de diffusion pris en charge.

Le tableau suivant répertorie les champs qui peuvent être inclus dans une notification de découverte. Dans le tableau, la colonne Champ de notification décrit (en italique) ou indique le nom d'un champ d'une notification. La colonne du champ d'événement Finding utilise la notation par points pour indiquer le nom du champ JSON correspondant à un EventBridge événement de recherche. La colonne Description décrit les données stockées dans le champ.

Champ de notification	Recherche d'un champ d'événement	Description
Titre du message	`detail.type`	Le type de découverte. Par exemple, `Policy:IAMUser/S3BucketPublic` ou `Sensitive Data:S3Object/Financial` .
Récapitulatif	`detail.title`	La courte description de la découverte. Par exemple : `The S3 object contains`

Champ de notification	Recherche d'un champ d'événement	Description
		`financial informati on.`
Description	`detail.description`	Description complète de la découverte. Par exemple : `The S3 object contains financial information such as bank account numbers or credit card numbers.`
Sévérité	`detail.severity.de scription`	La représentation qualitati ve de la gravité du résultat :`Low`,`Medium`, ou`High`.
ID de résultat	`detail.id`	Identifiant unique de la découverte.
Créé	`detail.createdAt`	La date et l'heure auxquelles
Mis à jour	`detail.updatedAt`	La date et l'heure auxquelles Pour les résultats de données sensibles, cette valeur est identique à celle du champ Created (`detail.cr eatedAt`). Toutes les données sensibles sont considérées comme nouvelles (uniques).
Compartiment S3	`detail.resourcesAf fected.s3Bucket.arn`	L'Amazon Resource Name (ARN) du compartiment S3.

Champ de notification	Recherche d'un champ d'événement	Description
Objet S3	`detail.resourcesAffected.s3Object.path`	Le nom (clé) de l'objet S3 concerné, y compris le nom du compartiment qui stocke l'objet et, le cas échéant, le préfixe de l'objet. Ce champ n'est pas inclus dans les notifications relatives aux résultats des politiques.

Champ de notification	Recherche d'un champ d'événement	Description

Détections de données sensibles	`detail.classificationDetails.result.sensitiveData.detections...`
	
	Et/ou
	
	`detail.classificationDetails.result.customDataIdentifiers.detections...`
		Il s'agit d'une concaténation de plusieurs champs lors d'un événement visant à détecter des données sensibles. Ce champ n'est pas inclus dans les notifications relatives aux résultats des politiques.
		
		Si un identifiant de données gérées a détecté les données sensibles, ce champ indique la catégorie, le type et le nombre (`count`) d'occurrences des données sensibles détectées. Par exemple : `PERSONAL_INFORMATION: USA_SOCIAL_SECURITY_NUMBER 100 occurrences .`
		
		Si un identifiant de données personnalisé a détecté les données sensibles, ce champ indique le nom de l'identifiant de données personnalisé et le nombre (`count`) d'occurrences des données sensibles détectées. Par exemple : `Employee ID 20 occurrences .`
		
		Si une découverte fait état de plusieurs types de données sensibles, la notification

Champ de notification	Recherche d'un champ d'événement	Description
		inclut des données pour un maximum de quatre types. Les données sont d'abord renseignées par tout identifiant de données personnalisé applicable, puis par tout identifiant de données gérées applicable.

Modification des paramètres de notifications utilisateur AWS pour les résultats d'Amazon Macie

Vous pouvez modifier vos paramètres de notifications utilisateur AWS pour les résultats d'Amazon Macie à tout moment. Pour ce faire, modifiez la configuration des notifications dans Notifications utilisateur. Pour savoir comment procéder, consultez la section Gestion des configurations de notifications dans le Guide de l'utilisateur AWS User Notifications.

Si vous avez plusieurs configurations de notification pour les résultats de Macie, la modification des paramètres d'une configuration n'affecte pas les paramètres des autres configurations. Vous pouvez modifier toutes vos configurations ou uniquement certaines d'entre elles.

Désactivation des notifications utilisateur AWS pour les résultats d'Amazon Macie

Pour arrêter de générer et de recevoir des notifications provenant d'AWS User Notifications pour les résultats d'Amazon Macie, supprimez la configuration des notifications dans Notifications utilisateur. Pour savoir comment procéder, consultez la section Gestion des configurations de notifications dans le Guide de l'utilisateur AWS User Notifications.

Si vous avez plusieurs configurations de notification pour les résultats de Macie, la suppression d'une configuration n'affecte pas les autres configurations. Vous pouvez supprimer toutes vos configurations ou uniquement certaines d'entre elles.

Schéma EventBridge d'événement Amazon pour les résultats d'Amazon Macie

Pour faciliter l'intégration avec d'autres applications, services et systèmes, tels que les systèmes de surveillance ou de gestion des événements, Amazon Macie publie automatiquement les résultats sur Amazon EventBridge sous forme d'événements. EventBridge, anciennement Amazon CloudWatch Events, est un service de bus d'événements sans serveur qui fournit un flux de données en temps réel provenant d'applications et d'autres entités Services AWS à des cibles telles que AWS Lambda les fonctions, les rubriques Amazon Simple Notification Service et les flux Amazon Kinesis. Pour en savoir plus EventBridge, consultez le guide de EventBridge l'utilisateur Amazon.

> **Note**
>
> Si vous utilisez actuellement CloudWatch Events, notez que EventBridge et CloudWatch Events sont le même service sous-jacent et la même API. Cependant, il EventBridge inclut des fonctionnalités supplémentaires qui vous permettent de recevoir des événements provenant d'applications SaaS (Software as a Service) et de vos propres applications. Le service sous-jacent et l'API étant identiques, le schéma des événements pour les résultats de Macie est également le même.

Macie publie automatiquement des événements pour toutes les nouvelles découvertes et les occurrences ultérieures de conclusions de politiques existantes, à l'exception des conclusions qui sont archivées automatiquement par une règle de suppression. Les événements sont des objets JSON conformes au EventBridge schéma des AWS événements. Chaque événement contient une représentation JSON d'une découverte particulière. Les données étant structurées sous la forme d'un EventBridge événement, vous pouvez plus facilement surveiller, traiter et agir en fonction d'une découverte en utilisant d'autres applications, services et outils. Pour plus de détails sur comment et quand Macie publie des événements pour obtenir des résultats, voirConfiguration des paramètres de publication pour les résultats.

Rubriques

Schéma d'événement

L'exemple suivant montre le schéma d'un EventBridge événement Amazon pour une découverte Amazon Macie. Pour obtenir une description détaillée des champs qui peuvent être inclus dans un événement de recherche, consultez la section Conclusions du manuel de référence des API Amazon Macie. La structure et les champs d'un événement de recherche sont étroitement liés à l'objet de recherche de l'API Amazon Macie.

```
{
    "version": "0",
    "id": "event ID",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "Compte AWS ID (string)",
    "time": "event timestamp (string)",
    "region": "Région AWS (string)",
    "resources": [
        <-- ARNs of the resources involved in the event -->
    ],
    "detail": {
        <-- Details of a policy or sensitive data finding -->
    },
    "policyDetails": null, <-- Additional details of a policy finding or null for a
 sensitive data finding -->
    "sample": Boolean,
    "archived": Boolean
}
```

Exemple d'événement pour un résultat de stratégie

L'exemple suivant utilise des exemples de données pour démontrer la structure et la nature des objets et des champs lors d'un EventBridge événement Amazon afin de déterminer une politique.

Dans cet exemple, l'événement signale une occurrence ultérieure d'une constatation de politique existante : les paramètres de blocage de l'accès public ont été désactivés pour un compartiment S3. Les champs et valeurs suivants peuvent vous aider à déterminer si tel est le cas :

- Le champ `type` est défini sur `Policy:IAMUser/S3BlockPublicAccessDisabled`.
- Les champs `updatedAt` et `createdAt` ont des valeurs différentes. Cela indique que l'événement signale une occurrence ultérieure d'une constatation de politique existante. Les valeurs de ces champs seraient identiques si l'événement signalait un nouveau résultat.

- Le `count` champ est défini sur2, ce qui indique qu'il s'agit de la deuxième occurrence du résultat.
- Le champ `category` est défini sur `POLICY`.
- La valeur du champ `classificationDetails` est `null`, ce qui permet de différencier cet événement pour un résultat de stratégie d'un événement pour un résultat de données sensibles. Pour un résultat de données sensibles, cette valeur serait un ensemble d'objets et de champs fournissant des informations sur les données sensibles et sur la manière dont elles ont été trouvées.

Notez également que la valeur du champ `sample` est `true`. Cette valeur indique qu'il s'agit d'un exemple d'événement utilisé dans la documentation.

```
{
    "version": "0",
    "id": "0948ba87-d3b8-c6d4-f2da-732a1example",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "123456789012",
    "time": "2021-04-30T23:12:15Z",
    "region":"us-east-1",
    "resources": [],
    "detail": {
        "schemaVersion": "1.0",
        "id": "64b917aa-3843-014c-91d8-937ffexample",
        "accountId": "123456789012",
        "partition": "aws",
        "region": "us-east-1",
        "type": "Policy:IAMUser/S3BlockPublicAccessDisabled",
        "title": "Block public access settings are disabled for the S3 bucket",
        "description": "All bucket-level block public access settings were disabled for
 the S3 bucket. Access to the bucket is controlled by account-level block public access
 settings, access control lists (ACLs), and the bucket's bucket policy.",
        "severity": {
            "score": 3,
            "description": "High"
        },
        "createdAt": "2021-04-29T15:46:02Z",
        "updatedAt": "2021-04-30T23:12:15Z",
        "count": 2,
        "resourcesAffected": {
            "s3Bucket": {
                "arn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
```

```
                "name": "DOC-EXAMPLE-BUCKET1",
                "createdAt": "2020-04-03T20:46:56.000Z",
                "owner":{
                    "displayName": "johndoe",
                    "id":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example"
                },
                "tags": [
                    {
                        "key": "Division",
                        "value": "HR"
                    },
                    {
                        "key": "Team",
                        "value": "Recruiting"
                    }
                ],
                "defaultServerSideEncryption": {
                    "encryptionType": "aws:kms",
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "publicAccess": {
                    "permissionConfiguration": {
                        "bucketLevelPermissions": {
                            "accessControlList": {
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "bucketPolicy": {
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "blockPublicAccess": {
                                "ignorePublicAcls": false,
                                "restrictPublicBuckets": false,
                                "blockPublicAcls": false,
                                "blockPublicPolicy": false
                            }
                        },
                        "accountLevelPermissions": {
                            "blockPublicAccess": {
                                "ignorePublicAcls": true,
                                "restrictPublicBuckets": true,
```

```
                                "blockPublicAcls": true,
                                "blockPublicPolicy": true
                            }
                        }
                    },
                    "effectivePermission": "NOT_PUBLIC"
                },
                "allowsUnencryptedObjectUploads": "FALSE"
            },
            "s3Object": null
        },
        "category": "POLICY",
        "classificationDetails": null,
        "policyDetails": {
            "action": {
                "actionType": "AWS_API_CALL",
                "apiCallDetails": {
                    "api": "PutBucketPublicAccessBlock",
                    "apiServiceName": "s3.amazonaws.com",
                    "firstSeen": "2021-04-29T15:46:02.401Z",
                    "lastSeen": "2021-04-30T23:12:15.401Z"
                }
            },
            "actor": {
                "userIdentity": {
                    "type": "AssumedRole",
                    "assumedRole": {
                        "principalId": "AROA1234567890EXAMPLE:AssumedRoleSessionName",
                        "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/
MySessionName",
                        "accountId": "111122223333",
                        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                        "sessionContext": {
                            "attributes": {
                                "mfaAuthenticated": false,
                                "creationDate": "2021-04-29T10:25:43.511Z"
                            },
                            "sessionIssuer": {
                                "type": "Role",
                                "principalId": "AROA1234567890EXAMPLE",
                                "arn": "arn:aws:iam::123456789012:role/
RoleToBeAssumed",
                                "accountId": "123456789012",
                                "userName": "RoleToBeAssumed"
```

```
                            }
                        }
                    },
                    "root": null,
                    "iamUser": null,
                    "federatedUser": null,
                    "awsAccount": null,
                    "awsService": null
                },
                "ipAddressDetails":{
                    "ipAddressV4": "192.0.2.0",
                    "ipOwner": {
                        "asn": "-1",
                        "asnOrg": "ExampleFindingASNOrg",
                        "isp": "ExampleFindingISP",
                        "org": "ExampleFindingORG"
                    },
                    "ipCountry": {
                        "code": "US",
                        "name": "United States"
                    },
                    "ipCity": {
                        "name": "Ashburn"
                    },
                    "ipGeoLocation": {
                        "lat": 39.0481,
                        "lon": -77.4728
                    }
                },
                "domainDetails": null
            }
        },
        "sample": true,
        "archived": false
    }
}
```


Exemple d'événement pour un résultat de données sensibles

L'exemple suivant utilise des exemples de données pour démontrer la structure et la nature des objets et des champs dans un EventBridge événement Amazon afin de trouver des données sensibles.

Dans cet exemple, l'événement signale une nouvelle découverte de données sensibles : Amazon Macie a détecté plusieurs catégories de données sensibles dans un objet S3. Les champs et valeurs suivants peuvent vous aider à déterminer que c'est le cas :

- Le champ `type` est défini sur `SensitiveData:S3Object/Multiple`.
- Les champs `updatedAt` et `createdAt` ont les mêmes valeurs. Contrairement aux résultats de stratégie, c'est toujours le cas pour les résultats de données sensibles. Toutes les découvertes relatives à des données sensibles sont considérées comme nouvelles.
- Le champ `count` est défini sur 1, ce qui indique qu'il s'agit d'un nouveau résultat. Contrairement aux résultats de stratégie, c'est toujours le cas pour les résultats de données sensibles. Toutes les données sensibles découvertes sont considérées comme uniques (nouvelles).
- Le champ `category` est défini sur `CLASSIFICATION`.
- La valeur du champ `policyDetails` est `null`, ce qui permet de différencier cet événement pour un résultat de données sensibles d'un événement pour un résultat de stratégie. Pour une constatation de politique, cette valeur serait un ensemble d'objets et de champs fournissant des informations sur une violation potentielle des politiques ou un problème de sécurité ou de confidentialité d'un compartiment S3.

Notez également que la valeur du champ `sample` est `true`. Cette valeur indique qu'il s'agit d'un exemple d'événement utilisé dans la documentation.


```
{
    "version": "0",
    "id": "14ddd0b1-7c90-b9e3-8a68-6a408example",
    "detail-type": "Macie Finding",
    "source": "aws.macie",
    "account": "123456789012",
    "time": "2022-04-20T08:19:10Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "schemaVersion": "1.0",
        "id": "4ed45d06-c9b9-4506-ab7f-18a57example",
        "accountId": "123456789012",
        "partition": "aws",
        "region": "us-east-1",
        "type": "SensitiveData:S3Object/Multiple",
        "title": "The S3 object contains multiple categories of sensitive data",
```

```
        "description": "The S3 object contains more than one category of sensitive
 data.",
        "severity": {
            "score": 3,
            "description": "High"
        },
        "createdAt": "2022-04-20T18:19:10Z",
        "updatedAt": "2022-04-20T18:19:10Z",
        "count": 1,
        "resourcesAffected": {
            "s3Bucket": {
                "arn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
                "name": "DOC-EXAMPLE-BUCKET2",
                "createdAt": "2020-05-15T20:46:56.000Z",
                "owner": {
                    "displayName": "johndoe",
                    "id":
 "7009a8971cd538e11f6b6606438875e7c86c5b672f46db45460ddcd08example"
                },
                "tags":[
                    {
                        "key":"Division",
                        "value":"HR"
                    },
                    {
                        "key":"Team",
                        "value":"Recruiting"
                    }
                ],
                "defaultServerSideEncryption": {
                    "encryptionType": "aws:kms",
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "publicAccess": {
                    "permissionConfiguration": {
                        "bucketLevelPermissions": {
                            "accessControlList": {
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
                            },
                            "bucketPolicy":{
                                "allowsPublicReadAccess": false,
                                "allowsPublicWriteAccess": false
```

```
                            },
                            "blockPublicAccess": {
                                "ignorePublicAcls": true,
                                "restrictPublicBuckets": true,
                                "blockPublicAcls": true,
                                "blockPublicPolicy": true
                            }
                        },
                        "accountLevelPermissions": {
                            "blockPublicAccess": {
                                "ignorePublicAcls": false,
                                "restrictPublicBuckets": false,
                                "blockPublicAcls": false,
                                "blockPublicPolicy": false
                            }
                        }
                    },
                    "effectivePermission": "NOT_PUBLIC"
                },
                "allowsUnencryptedObjectUploads": "TRUE"
            },
            "s3Object":{
                "bucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET2",
                "key": "2022 Sourcing.csv",
                "path": "DOC-EXAMPLE-BUCKET2/2022 Sourcing.csv",
                "extension": "csv",
                "lastModified": "2022-04-19T22:08:25.000Z",
                "versionId": "",
                "serverSideEncryption": {
                    "encryptionType": "aws:kms",
                    "kmsMasterKeyId": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab"
                },
                "size": 4750,
                "storageClass": "STANDARD",
                "tags":[
                    {
                        "key":"Division",
                        "value":"HR"
                    },
                    {
                        "key":"Team",
                        "value":"Recruiting"
                    }
```

```
                ],
                "publicAccess": false,
                "etag": "6bb7fd4fa9d36d6b8fb8882caexample"
            }
        },
        "category": "CLASSIFICATION",
        "classificationDetails": {
            "jobArn": "arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample",
            "jobId": "3ce05dbb7ec5505def334104bexample",
            "result": {
                "status": {
                    "code": "COMPLETE",
                    "reason": null
                },
                "sizeClassified": 4750,
                "mimeType": "text/csv",
                "additionalOccurrences": true,
                "sensitiveData": [
                    {
                        "category": "PERSONAL_INFORMATION",
                        "totalCount": 65,
                        "detections": [
                            {
                                "type": "USA_SOCIAL_SECURITY_NUMBER",
                                "count": 30,
                                "occurrences": {
                                    "lineRanges": null,
                                    "offsetRanges": null,
                                    "pages": null,
                                    "records": null,
                                    "cells": [
                                        {
                                            "row": 2,
                                            "column": 1,
                                            "columnName": "SSN",
                                            "cellReference": null
                                        },
                                        {
                                            "row": 3,
                                            "column": 1,
                                            "columnName": "SSN",
                                            "cellReference": null
                                        },
```

```
                                {
                                    "row": 4,
                                    "column": 1,
                                    "columnName": "SSN",
                                    "cellReference": null
                                }
                            ]
                        }
                    },
                    {
                        "type": "NAME",
                        "count": 35,
                        "occurrences": {
                            "lineRanges": null,
                            "offsetRanges": null,
                            "pages": null,
                            "records": null,
                            "cells": [
                                {
                                    "row": 2,
                                    "column": 3,
                                    "columnName": "Name",
                                    "cellReference": null
                                },
                                {
                                    "row": 3,
                                    "column": 3,
                                    "columnName": "Name",
                                    "cellReference": null
                                }
                            ]
                        }
                    }
                ]
            },
            {
                "category": "FINANCIAL_INFORMATION",
                "totalCount": 30,
                "detections": [
                    {
                        "type": "CREDIT_CARD_NUMBER",
                        "count": 30,
                        "occurrences": {
                            "lineRanges": null,
```

```
                                    "offsetRanges": null,
                                    "pages": null,
                                    "records": null,
                                    "cells": [
                                        {
                                            "row": 2,
                                            "column": 14,
                                            "columnName": "CCN",
                                            "cellReference": null
                                        },
                                        {
                                            "row": 3,
                                            "column": 14,
                                            "columnName": "CCN",
                                            "cellReference": null
                                        }
                                    ]
                                }
                            }
                        ]
                    }
                ],
                "customDataIdentifiers": {
                    "totalCount": 0,
                    "detections": []
                }
            },
            "detailedResultsLocation": "s3://macie-data-discovery-results/
AWSLogs/123456789012/Macie/us-east-1/3ce05dbb7ec5505def334104bexample/
d48bf16d-0deb-3e49-9d8c-d407cexample.jsonl.gz",
            "originType": "SENSITIVE_DATA_DISCOVERY_JOB"
        },
        "policyDetails": null,
        "sample": true,
        "archived": false
    }
}
```

Prévision et surveillance des coûts d'Amazon Macie

Pour vous aider à prévoir et à surveiller les coûts liés à l'utilisation d'Amazon Macie, Macie calcule et fournit une estimation des coûts d'utilisation de votre compte. À l'aide de ces données, vous pouvez déterminer s'il convient d'ajuster votre utilisation du service ou les quotas de votre compte. Si vous participez actuellement à un essai gratuit de 30 jours de Macie, vous pouvez utiliser ces données pour estimer les coûts d'utilisation de Macie après la fin de l'essai gratuit. Vous pouvez également vérifier le statut de votre essai.

Vous pouvez consulter vos coûts d'utilisation estimés sur la console Amazon Macie et y accéder par programmation à l'aide de l'API Amazon Macie. Si vous êtes l'administrateur Macie d'une organisation, vous pouvez consulter et accéder à la fois aux données agrégées de votre organisation et aux ventilations des données relatives aux comptes de votre organisation.

Outre les coûts d'utilisation estimés fournis par Macie, vous pouvez consulter et surveiller vos coûts réels en utilisant AWS Billing and Cost Management. AWS Billing and Cost Management fournit des fonctionnalités conçues pour vous aider à suivre et à analyser vos coûts et à Services AWS gérer les budgets de votre compte ou de votre organisation. Il fournit également des fonctionnalités qui peuvent vous aider à prévoir les coûts d'utilisation sur la base de données historiques. Pour en savoir plus, consultez le AWS Billing guide de l'utilisateur.

Rubriques

Comprendre comment les coûts d'utilisation estimés sont calculés pour Amazon Macie

La tarification d'Amazon Macie est basée sur les dimensions suivantes.

Surveillance des contrôles préventifs

Ces coûts sont liés à la gestion d'un inventaire de vos compartiments à usage général Amazon Simple Storage Service (Amazon S3), ainsi qu'à l'évaluation et à la surveillance de ces

compartiments à des fins de sécurité et de contrôle d'accès. Pour plus d'informations, consultez Comment Macie surveille la sécurité des données Amazon S3.

Vous êtes débité en fonction du nombre total de compartiments S3 à usage général que Macie surveille pour votre compte. Les frais sont calculés au prorata par jour.

Surveillance des objets pour la découverte automatique des données sensibles

Ces coûts découlent de la surveillance et de l'évaluation de votre inventaire de compartiments S3 afin d'identifier les objets S3 éligibles à une analyse par découverte automatique de données sensibles. Pour plus d'informations, consultez Comment fonctionne la découverte automatique des données sensibles.

Vous êtes débité en fonction du nombre total d'objets S3 contenus dans des compartiments à usage général que Macie surveille pour votre compte. Les frais sont calculés au prorata par jour.

Analyse d'objets grâce à des tâches de découverte de données sensibles et à une découverte automatique de données sensibles

Ces coûts découlent de l'analyse des objets S3 et de la génération de rapports sur les données sensibles que Macie trouve dans ces objets. Cela inclut les analyses et les rapports par le biais de tâches de découverte de données sensibles et de découverte automatique de données sensibles. Pour plus d'informations, consultez Découverte de données sensibles.

Vous êtes facturé en fonction de la quantité de données non compressées que Macie analyse dans les objets S3. Les objets que Macie ne peut pas analyser sont gratuits pour des raisons telles que l'utilisation d'une classe de stockage Amazon S3 non prise en charge, l'utilisation d'un format de fichier ou de stockage non pris en charge ou les paramètres d'autorisation. De plus, ces coûts ne varient pas en fonction du nombre de découvertes de données sensibles produites par vos tâches ou par la découverte automatique de données sensibles.

Pour gérer les coûts liés à la découverte automatisée des données sensibles, vous pouvez exclure des compartiments S3 individuels des analyses. Par exemple, vous pouvez exclure les compartiments réputés répondre aux exigences de sécurité et de conformité de votre organisation. Si votre compte fait partie d'une organisation qui gère de manière centralisée plusieurs comptes Macie, une option supplémentaire consiste à activer ou désactiver de manière sélective la découverte automatique des données sensibles pour les comptes individuels de votre organisation. Pour plus d'informations, consultez Configuration de la découverte automatique des données sensibles.

Les coûts des tâches de découverte de données sensibles sont limités par le quota mensuel de découverte de données sensibles de votre compte. (Le quota par défaut est de 5 To de données.) Si une tâche est en cours d'exécution et que l'analyse des objets éligibles atteint ce quota, Macie suspend automatiquement la tâche jusqu'au début du mois civil suivant et le quota mensuel est redéfini pour votre compte, ou vous augmentez le quota pour votre compte.

Si vous êtes l'administrateur Macie d'une organisation, les coûts des tâches de découverte de données sensibles sont limités par le quota mensuel de découverte de données sensibles pour chaque compte pour lequel vous analysez les données. Le quota d'un compte membre définit la quantité maximale de données que vos offres d'emploi et celles associées au compte membre peuvent analyser pour le compte au cours d'un mois civil. Si une tâche est en cours d'exécution et que l'analyse des objets éligibles atteint ce quota pour un compte membre, Macie arrête d'analyser les objets dans les compartiments détenus par le compte. Lorsque Macie a fini d'analyser les objets pour tous les autres comptes n'ayant pas atteint le quota, Macie interrompt automatiquement le travail. S'il s'agit d'une tâche ponctuelle, Macie reprend automatiquement la tâche au début du mois civil suivant ou le quota est augmenté pour tous les comptes concernés, selon la première éventualité. S'il s'agit d'une tâche périodique, Macie reprend automatiquement la tâche au début de la prochaine exécution ou au début du mois civil suivant, selon la première éventualité. Si une course planifiée commence avant le début du mois civil suivant ou si le quota est augmenté pour un compte concerné, Macie n'analyse pas les objets contenus dans les compartiments détenus par le compte.

> **Tip**
>
> Pour obtenir des conseils utiles sur la gestion ou la réduction des coûts liés à la découverte de données sensibles, consultez le billet de blog Comment utiliser Amazon Macie pour réduire les coûts liés à la découverte de données sensibles sur le blog sur la AWS sécurité.

Pour obtenir des informations détaillées et des exemples de coûts d'utilisation, consultez la tarification d'Amazon Macie.

Lorsque vous utilisez Macie pour examiner vos coûts d'utilisation estimés, il est important de comprendre comment les estimations de coûts sont calculées. Éléments à prendre en compte :

- Les estimations sont présentées en dollars américains et ne concernent Région AWS que le courant actuel. Si vous utilisez Macie dans plusieurs régions, les données ne sont pas agrégées pour toutes les régions dans lesquelles vous utilisez Macie.
- Sur la console, les estimations sont incluses pour le mois civil en cours à ce jour. Si vous interrogez les données par programmation à l'aide de l'API Amazon Macie, vous pouvez choisir une plage de temps incluse pour les estimations. Il peut s'agir d'une période continue des 30 jours précédents ou du mois civil en cours à ce jour.
- Les estimations ne tiennent pas compte de toutes les remises susceptibles de s'appliquer à votre compte. L'exception concerne les remises qui découlent des niveaux de tarification régionaux en fonction du volume, comme décrit dans la section Tarification d'Amazon Macie. Si votre compte est éligible à ce type de réduction, les estimations reflètent cette réduction.
- Si vous êtes l'administrateur Macie d'une organisation, les estimations ne reflètent pas les remises combinées sur le volume d'utilisation pour votre organisation. Pour plus d'informations sur ces remises, consultez la section Réductions sur volume dans le guide de AWS Billing l'utilisateur.
- Pour le suivi du contrôle préventif, l'estimation est basée sur le coût quotidien moyen pour la plage de temps applicable. Le coût est calculé au prorata par jour.
- Pour la découverte automatisée de données sensibles, l'estimation globale est basée sur le coût quotidien moyen de la surveillance des objets (calculé au prorata par jour) et sur la quantité de données non compressées que Macie a analysées jusqu'à présent pendant la période applicable. Si vous êtes l'administrateur Macie d'une organisation et que vous activez la découverte automatique des données sensibles pour les comptes des membres, les coûts estimés de ces activités sont inclus dans les estimations pour chaque compte membre applicable.
- Pour les tâches de découverte de données sensibles, l'estimation est basée sur la quantité de données non compressées que vos tâches ont analysées jusqu'à présent pendant la période applicable. Si vous êtes l'administrateur Macie d'une organisation et que vous exécutez des tâches qui analysent les données des comptes des membres, les coûts estimés de ces tâches sont inclus dans l'estimation de chaque compte membre applicable.
- Si votre compte est un compte membre d'une organisation et que votre administrateur Macie effectue la découverte automatique de données sensibles ou exécute des tâches de découverte de données sensibles pour analyser vos données, les coûts estimés de ces activités sont inclus dans les estimations de votre compte.
- Les estimations n'incluent pas les coûts que vous encourez pour utiliser d'autres Services AWS fonctionnalités de Macie. Par exemple, vous pouvez utiliser la solution gérée par le client AWS KMS keys pour déchiffrer les objets S3 dont vous souhaitez inspecter les données sensibles.

Notez également que Macie propose un niveau mensuel gratuit pour l'analyse des objets S3 par le biais de tâches de découverte de données sensibles et de découverte automatique de données sensibles. Chaque mois, vous pouvez analyser gratuitement jusqu'à 1 Go de données afin de découvrir et de signaler des données sensibles dans des objets S3. Si plus de 1 Go de données sont analysés au cours d'un mois donné, des frais de découverte de données sensibles commencent à être facturés sur votre compte après le premier Go de données. Si moins de 1 Go de données sont analysés au cours d'un mois donné, l'allocation restante n'est pas reportée au mois suivant. Si votre compte fait partie d'une organisation avec facturation consolidée, le niveau gratuit s'applique à la quantité combinée de données analysées pour votre organisation. En d'autres termes, l'analyse gratuite de jusqu'à 1 Go de données par mois pour tous les comptes de votre organisation est gratuite.

Révision des coûts d'utilisation estimés pour Amazon Macie

Pour consulter vos coûts d'utilisation estimés actuels pour Amazon Macie, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie. La console et l'API fournissent des estimations des coûts pour les dimensions de tarification de Macie. Si vous participez actuellement à un essai gratuit de 30 jours, vous pouvez utiliser ces données pour estimer les coûts d'utilisation de Macie après la fin de votre essai gratuit. Pour plus d'informations sur les dimensions tarifaires et les considérations relatives à Macie, consultezComprendre comment les coûts d'utilisation estimés sont calculés. Pour obtenir des informations détaillées et des exemples de coûts d'utilisation, consultez la tarification d'Amazon Macie.

À Macie, les coûts d'utilisation estimés sont indiqués en dollars américains et ne s'appliquent qu'aux coûts actuels Région AWS. Si vous utilisez la console pour consulter les données, les estimations de coûts concernent le mois civil en cours (inclus). Si vous interrogez les données par programmation à l'aide de l'API Amazon Macie, vous pouvez spécifier une plage de temps inclusive pour les estimations, soit une période continue des 30 jours précédents, soit le mois civil en cours à ce jour.

Rubriques

- Révision des coûts d'utilisation estimés sur la console Amazon Macie
- Interrogation des coûts d'utilisation estimés à l'aide de l'API Amazon Macie

Révision des coûts d'utilisation estimés sur la console Amazon Macie

Sur la console Amazon Macie, les estimations de coûts sont organisées comme suit :

- Surveillance préventive des contrôles : il s'agit du coût estimé de la gestion d'un inventaire de vos compartiments à usage général Amazon Simple Storage Service (Amazon S3), ainsi que de l'évaluation et de la surveillance des compartiments à des fins de sécurité et de contrôle d'accès.
- Tâches de découverte de données sensibles : il s'agit du coût estimé des tâches de découverte de données sensibles que vous avez exécutées.
- Découverte automatisée des données sensibles : il s'agit des coûts estimés liés à la découverte automatique des données sensibles. Cela inclut la surveillance et l'évaluation de votre inventaire de compartiments S3 afin d'identifier les objets S3 éligibles à l'analyse. Cela inclut également l'analyse des objets éligibles et la production de rapports sur les données sensibles, les statistiques, les conclusions et d'autres types de résultats. Pour consulter ces estimations, votre compte doit être le compte administrateur Macie d'une organisation ou un compte Macie autonome.

Suivez ces étapes pour consulter vos coûts d'utilisation estimés à l'aide de la console Amazon Macie.

Pour consulter vos coûts d'utilisation estimés sur la console

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez consulter vos coûts estimés.
3. Dans le panneau de navigation, choisissez Utilisateurs.

Si vous avez un compte Macie autonome ou si votre compte est un compte membre d'une organisation, la page Utilisation affiche une ventilation des coûts d'utilisation estimés pour votre compte.

Si vous êtes l'administrateur Macie d'une organisation, la page Utilisation répertorie les comptes de votre organisation. Dans le tableau :

- Quota de service — Tâches — Il s'agit du quota mensuel actuel pour exécuter des tâches de découverte de données sensibles afin d'analyser des objets S3 dans des compartiments détenus par un compte.
- Essai gratuit — Ces champs indiquent si un compte participe actuellement à l'essai gratuit pour la surveillance des contrôles préventifs ou la découverte automatisée de données sensibles. Un champ d'essai gratuit est vide si l'essai gratuit applicable est terminé pour un compte.
- Total — Il s'agit du coût total estimé pour un compte.

La section Coûts estimés indique le coût total estimé pour votre organisation et une ventilation de ces coûts. Pour consulter la ventilation des coûts estimés pour un compte spécifique de votre organisation, sélectionnez le compte dans le tableau. La section Coûts estimés affiche ensuite cette ventilation. Pour afficher ces données pour un autre compte, sélectionnez le compte dans le tableau. Pour effacer votre sélection de compte, choisissez X à côté de l'identifiant du compte.

Interrogation des coûts d'utilisation estimés à l'aide de l'API Amazon Macie

Pour demander vos coûts d'utilisation estimés par programmation, vous pouvez utiliser les opérations suivantes de l'API Amazon Macie :

- GetUsageTotals— Cette opération renvoie le total des coûts d'utilisation estimés pour votre compte, regroupés par indicateur d'utilisation. Si vous êtes l'administrateur Macie d'une organisation, cette opération renvoie des estimations de coûts agrégées pour tous les comptes de votre organisation. Pour en savoir plus sur cette opération, consultez la section Totaux d'utilisation dans le manuel Amazon Macie API Reference.
- GetUsageStatistics— Cette opération renvoie les statistiques d'utilisation et les données associées à votre compte, regroupées par compte puis par métrique d'utilisation. Les données incluent les coûts d'utilisation estimés totaux et les quotas du compte courant. Le cas échéant, il indique également la date de début de votre essai gratuit de 30 jours pour Macie et pour la découverte automatique de données sensibles. Si vous êtes l'administrateur Macie d'une organisation, cette opération renvoie une ventilation des données pour tous les comptes de votre organisation. Vous pouvez personnaliser votre requête en triant et en filtrant les résultats de la requête. Pour en savoir plus sur cette opération, consultez les statistiques d'utilisation dans le manuel Amazon Macie API Reference.

Lorsque vous utilisez l'une ou l'autre opération, vous pouvez éventuellement spécifier une plage de temps inclusive pour les données. Cette plage de temps peut être une plage de temps continue des 30 jours précédents (`PAST_30_DAYS`) ou du mois civil en cours (`MONTH_TO_DATE`). Si vous ne spécifiez aucun intervalle de temps, Macie renvoie les données des 30 jours précédents.

Les exemples suivants montrent comment interroger les coûts d'utilisation estimés et les statistiques à l'aide de AWS Command Line Interface (AWS CLI). Vous pouvez également interroger les données en utilisant la version actuelle d'un autre outil de ligne de AWS commande ou d'un AWS SDK, ou en envoyant des requêtes HTTPS directement à Macie. Pour plus d'informations sur AWS les outils et les SDK, consultez la section Outils sur AWS lesquels vous pouvez vous appuyer.

Exemples

Exemple 1 : Interrogation du total des coûts d'utilisation estimés

Pour demander le total des coûts d'utilisation estimés à l'aide de AWS CLI, exécutez la get-usage-totalscommande et spécifiez éventuellement une plage de temps pour les données. Par exemple :

```
C:\> aws macie2 get-usage-totals --time-range MONTH_TO_DATE
```

Where *MONTH_TO_DATE*indique le mois calendaire en cours comme plage de temps pour les données.

Si la commande s'exécute correctement, vous recevez une sortie similaire à ce qui suit.

```
{
    "timeRange": "MONTH_TO_DATE",
    "usageTotals": [
        {
            "currency": "USD",
            "estimatedCost": "153.45",
            "type": "SENSITIVE_DATA_DISCOVERY"
        },
        {
            "currency": "USD",
            "estimatedCost": "65.18",
            "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
        },
        {
            "currency": "USD",
            "estimatedCost": "1.51",
            "type": "DATA_INVENTORY_EVALUATION"
        },
        {
            "currency": "USD",
            "estimatedCost": "0.98",
            "type": "AUTOMATED_OBJECT_MONITORING"
        }
    ]
}
```

Où `estimatedCost` est le coût d'utilisation total estimé pour la métrique d'utilisation associée (`type`) :

- `SENSITIVE_DATA_DISCOVERY`, pour analyser des objets S3 avec des tâches de découverte de données sensibles.
- `AUTOMATED_SENSITIVE_DATA_DISCOVERY`, pour analyser des objets S3 grâce à la découverte automatique de données sensibles.
- `DATA_INVENTORY_EVALUATION`, pour surveiller et évaluer les compartiments S3 à usage général à des fins de sécurité et de contrôle d'accès.
- `AUTOMATED_OBJECT_MONITORING`, pour évaluer et surveiller votre inventaire de compartiments S3 afin d'identifier les objets S3 susceptibles d'être analysés par découverte automatique de données sensibles.

Exemple 2 : Interrogation des statistiques d'utilisation

Pour consulter les statistiques d'utilisation à l'aide de AWS CLI, exécutez la get-usage-statisticscommande. Vous pouvez éventuellement trier, filtrer et spécifier une plage de temps pour les résultats de la requête. L'exemple suivant permet de récupérer les statistiques d'utilisation d'un compte administrateur Macie au cours des 30 derniers jours. Les résultats sont triés par ordre croissant par Compte AWS ID.

Pour Linux, macOS ou Unix, utilisez la barre oblique inverse (\) pour améliorer la lisibilité :

```
$ aws macie2 get-usage-statistics \
--sort-by '{"key":"accountId","orderBy":"ASC"}' \
--time-range PAST_30_DAYS
```

Pour Microsoft Windows, utilisez le caractère de continuation de ligne caret (^) pour améliorer la lisibilité :

```
C:\> aws macie2 get-usage-statistics ^
--sort-by={\"key\":\"accountId\",\"orderBy\":\"ASC\"} ^
--time-range PAST_30_DAYS
```

Où :

- *`AccountID`* indique le champ à utiliser pour trier les résultats.

- L'*ASC* est l'ordre de tri à appliquer aux résultats, en fonction de la valeur du champ spécifié (*AccountID*).
- *PAST_30_DAYS*indique les 30 jours précédents comme plage de temps pour les données.

Si la commande s'exécute correctement, Macie renvoie un `records` tableau. Le tableau contient un objet pour chaque compte inclus dans les résultats de la requête. Par exemple :


```
{
    "records": [
        {
            "accountId": "111122223333",
            "automatedDiscoveryFreeTrialStartDate": "2024-01-28T16:00:00+00:00",
            "freeTrialStartDate": "2020-05-20T12:26:36.917000+00:00",
            "usage": [
                {
                    "currency": "USD",
                    "estimatedCost": "1.51",
                    "type": "DATA_INVENTORY_EVALUATION"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "65.18",
                    "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "153.45",
                    "serviceLimit": {
                        "isServiceLimited": false,
                        "unit": "TERABYTES",
                        "value": 50
                    },
                    "type": "SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "0.98",
                    "type": "AUTOMATED_OBJECT_MONITORING"
                }
            ]
        },
        {
```

```
            "accountId": "444455556666",
            "automatedDiscoveryFreeTrialStartDate": "2024-01-28T16:00:00+00:00",
            "freeTrialStartDate": "2020-05-18T16:26:36.917000+00:00",
            "usage": [
                {
                    "currency": "USD",
                    "estimatedCost": "1.58",
                    "type": "DATA_INVENTORY_EVALUATION"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "63.13",
                    "type": "AUTOMATED_SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "145.12",
                    "serviceLimit": {
                        "isServiceLimited": false,
                        "unit": "TERABYTES",
                        "value": 50
                    },
                    "type": "SENSITIVE_DATA_DISCOVERY"
                },
                {
                    "currency": "USD",
                    "estimatedCost": "1.02",
                    "type": "AUTOMATED_OBJECT_MONITORING"
                }
            ]
        }
    ],
    "timeRange": "PAST_30_DAYS"
}
```


Où `estimatedCost` est le coût d'utilisation total estimé pour la métrique d'utilisation associée (`type`) pour un compte :

- `DATA_INVENTORY_EVALUATION`, pour surveiller et évaluer les compartiments S3 à usage général à des fins de sécurité et de contrôle d'accès.
- `AUTOMATED_SENSITIVE_DATA_DISCOVERY`, pour analyser des objets S3 grâce à la découverte automatique de données sensibles.

- `SENSITIVE_DATA_DISCOVERY`, pour analyser des objets S3 avec des tâches de découverte de données sensibles.
- `AUTOMATED_OBJECT_MONITORING`, pour évaluer et surveiller l'inventaire des compartiments S3 du compte afin d'identifier les objets S3 susceptibles d'être analysés par découverte automatique de données sensibles.

Participation à l'essai gratuit d'Amazon Macie

Lorsque vous activez Amazon Macie pour la première fois, vous êtes automatiquement Compte AWS inscrit à l'essai gratuit de 30 jours de Macie. Cela inclut les comptes de membres individuels d'une AWS Organizations organisation.

Pendant l'essai gratuit, l'utilisation gratuite de Macie dans un but spécifique Région AWS pour :

- Effectuez une surveillance préventive des contrôles : cela inclut la génération et la gestion d'un inventaire de vos compartiments à usage général Amazon Simple Storage Service (Amazon S3) dans la région. Cela inclut également l'évaluation et la surveillance des compartiments à des fins de sécurité et de contrôle d'accès.

  Pour plus d'informations, consultez Comment Macie surveille la sécurité des données Amazon S3.
- Effectuez une découverte automatisée des données sensibles : cela inclut la surveillance et l'évaluation de votre inventaire de compartiments S3 dans la région afin d'identifier les objets S3 éligibles à l'analyse. Cela inclut également l'analyse des objets éligibles et la production de rapports sur les données sensibles, les statistiques, les conclusions et d'autres types de résultats. Pour configurer et gérer cette fonctionnalité, votre compte doit être le compte administrateur Macie d'une organisation ou un compte Macie autonome. Si vous êtes l'administrateur Macie d'une organisation, vous pouvez utiliser cette fonctionnalité pour analyser les objets contenus dans les compartiments S3 détenus par vos comptes membres.

  Pour plus d'informations, consultez Comment fonctionne la découverte automatique des données sensibles.

Pour obtenir la liste des régions dans lesquelles Macie est actuellement disponible, consultez la section Points de terminaison et quotas Amazon Macie dans le. Références générales AWS

L'essai gratuit dure 30 jours consécutifs. Vous ne pouvez pas le mettre en pause une fois qu'il a démarré. À la fin de l'essai gratuit, des frais commencent à s'accumuler pour effectuer une

surveillance préventive des contrôles. Des frais commencent également à s'accumuler pour la découverte automatisée de données sensibles. Si vous êtes l'administrateur Macie d'une organisation, les frais s'accumulent, le cas échéant, pour chaque compte de votre organisation. Vous pouvez utiliser Macie pour consulter les ventilations des coûts d'utilisation estimés pour les comptes individuels de votre organisation.

> **Remarques**
>
> Au cours de l'essai gratuit, d'autres fonctionnalités de Macie peuvent vous être Services AWS facturées, par exemple l'utilisation d'objets S3 gérés AWS KMS keys par le client pour déchiffrer des objets S3 que vous souhaitez inspecter pour détecter la présence de données sensibles.
>
> L'essai gratuit n'inclut pas l'analyse des objets S3 par des tâches de découverte de données sensibles. Des frais vous seront facturés si vous créez et exécutez des tâches de découverte de données sensibles qui analysent plus de 1 Go de données non compressées pendant l'essai gratuit. (Macie propose un abonnement mensuel gratuit pour la découverte de données sensibles. Chaque mois, l'analyse d'un maximum de 1 Go de données non compressées dans des objets S3 est gratuite. Après le premier Go de données, les coûts s'accumulent.)

Pendant l'essai gratuit, vous pouvez vérifier l'état de votre essai et consulter les coûts d'utilisation estimés pour votre compte. Les estimations de coûts sont basées sur votre utilisation de Macie jusqu'à présent pendant l'essai gratuit. Ils peuvent vous aider à comprendre quels pourraient être certains de vos coûts d'utilisation après la fin de la période d'essai. Pour plus de détails sur le mode de calcul de ces valeurs par Macie, consultez. Comprendre comment les coûts d'utilisation estimés sont calculés

Pour vérifier votre statut et les coûts estimés pendant l'essai gratuit

Suivez ces étapes pour vérifier le statut de votre essai et consulter vos coûts d'utilisation estimés à l'aide de la console Amazon Macie. Vous pouvez également accéder à ces données par programmation en utilisant l'GetUsageStatisticsAPI Amazon Macie.

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez vérifier le statut de votre essai gratuit et vos coûts d'utilisation estimés.

3. Dans le panneau de navigation, choisissez Utilisateurs.

La page Utilisation indique le nombre de jours restants pour votre essai gratuit. Il présente également une ventilation de vos coûts d'utilisation estimés en dollars américains :

- Surveillance des contrôles préventifs : il s'agit du coût total prévu pour maintenir un inventaire de vos compartiments S3 à usage général, ainsi que pour évaluer et surveiller les compartiments à des fins de sécurité et de contrôle d'accès après la fin de l'essai gratuit.
- Tâches de découverte de données sensibles : il s'agit du coût total estimé de toutes les tâches de découverte de données sensibles que vous avez exécutées. Les tâches de découverte de données sensibles ne sont pas incluses dans l'essai gratuit.
- Découverte automatisée des données sensibles : il s'agit du coût total prévu pour effectuer la découverte automatique des données sensibles après la fin de l'essai gratuit, ventilés par dimension tarifaire (surveillance et analyse des objets). Pour consulter ces estimations, votre compte doit être le compte administrateur Macie d'une organisation ou un compte Macie autonome.

Si vous êtes l'administrateur Macie d'une organisation, la page Utilisation fournit des informations détaillées sur les comptes Macie de votre organisation. Dans le tableau :

- Quota de service — Tâches — Il s'agit du quota mensuel actuel pour exécuter des tâches de découverte de données sensibles afin d'analyser des objets S3 dans des compartiments détenus par un compte.
- Essai gratuit — Ces champs indiquent si un compte participe actuellement à l'essai gratuit pour la surveillance des contrôles préventifs ou la découverte automatisée de données sensibles. Un champ d'essai gratuit est vide si l'essai gratuit applicable est terminé pour un compte.
- Total — Il s'agit du coût total estimé pour un compte.

La section Coûts estimés indique les coûts estimés pour l'ensemble de votre organisation. Pour consulter la ventilation des coûts estimés pour un compte spécifique de votre organisation, sélectionnez le compte dans le tableau. La section Coûts estimés affiche ensuite cette ventilation. Pour afficher ces données pour un autre compte, sélectionnez le compte dans le tableau. Pour effacer votre sélection de compte, choisissez X à côté de l'identifiant du compte.

Remarques

Si un compte stocke plus de 150 To de données dans Amazon S3, les coûts estimés et réels du compte pour la découverte automatique de données sensibles peuvent être supérieurs aux prévisions de coûts fournies par Macie pendant l'essai gratuit de 30 jours. Cela est dû au fait que l'analyse des objets par découverte automatique de données sensibles est suspendue lorsque 150 Go de données non compressées ont été analysés pour un compte inscrit à l'essai gratuit. L'analyse des objets du compte reprend après la fin de l'essai gratuit. Pour obtenir de l'aide pour prévoir les coûts d'un compte stockant plus de 150 To de données dans Amazon S3, contactez AWS Support.

Pour gérer les coûts liés à la découverte automatique des données sensibles après la fin de l'essai gratuit, vous pouvez exclure des compartiments S3 individuels des analyses ultérieures. Si vous êtes l'administrateur Macie d'une organisation, une option supplémentaire consiste à activer ou désactiver de manière sélective la découverte automatique des données sensibles pour les comptes individuels de votre organisation. Pour de plus amples informations sur ces options, consultez Configuration de la découverte automatique des données sensibles.

Gestion de plusieurs comptes Amazon Macie

Si votre AWS environnement comporte plusieurs comptes, vous pouvez associer les comptes Amazon Macie à votre environnement et les gérer de manière centralisée en tant qu'organisation dans Macie. Grâce à cette configuration, un administrateur Macie désigné peut évaluer et surveiller le niveau de sécurité global du parc de données Amazon Simple Storage Service (Amazon S3) de votre organisation et découvrir des données sensibles dans les compartiments S3 de votre organisation. L'administrateur peut également effectuer diverses tâches de gestion et d'administration des comptes à grande échelle, telles que le suivi des coûts d'utilisation estimés et l'évaluation des quotas de comptes.

Dans Macie, une organisation se compose d'un compte administrateur Macie désigné et d'un ou plusieurs comptes membres associés. Vous pouvez associer les comptes de deux manières : en intégrant Macie à Macie AWS Organizations ou en envoyant et en acceptant des invitations d'adhésion dans Macie. Nous vous recommandons d'intégrer Macie ie ie ie ie ie ie ie ie ie ie ie AWS Organizations

AWS Organizationsest un service global de gestion de comptes qui permet aux AWS administrateurs de consolider et de gérer plusieurs comptes de manière centraliséeComptes AWS. Il inclut des capacités de facturation consolidée et de gestion de compte vous aidant à satisfaire les besoins budgétaires, de sécurité et de conformité de facturation consolidée et de gestion de compte vous aidant à satisfaire les besoins budgétaires, Il est proposé sans frais supplémentaires et s'intègre à plusieurs d'entre Services AWS eux, notamment Macie et AmazonGuardDuty. AWS Security Hub Pour en savoir plus, consultez le AWS Organizationsguide de l'utilisateur.

Si vous préférez gérer de manière centralisée plusieurs comptes Macie sans les utiliserAWS Organizations, vous pouvez utiliser des invitations d'adhésion à la place. Si vous envoyez une invitation et qu'elle est acceptée par un autre compte, votre compte devient le compte administrateur Macie de l'autre compte. Si vous recevez et acceptez une invitation, votre compte devient un compte de membre Macie et le compte administrateur de Macie peut accéder à certains paramètres, données et ressources de votre compte Macie et les gérer.

Rubriques

Comprendre la relation entre les comptes d'administrateur et de membre d'Amazon Macie

Si vous gérez de manière centralisée plusieurs comptes Amazon Macie en tant qu'organisation, l'administrateur Macie a accès aux données d'inventaire Amazon Simple Storage Service (Amazon S3), aux conclusions des politiques, ainsi qu'à certains paramètres et ressources Macie pour les comptes membres associés. L'administrateur peut également activer la découverte automatique des données sensibles et exécuter des tâches de découverte de données sensibles pour détecter les données sensibles dans les compartiments S3 détenus par les comptes membres. Support pour des tâches spécifiques varie selon qu'un compte administrateur Macie est associé à un compte membre via AWS Organizations ou sur invitation.

Le tableau suivant fournit des détails sur la relation entre les comptes administrateur et membre de Macie. Il indique les autorisations par défaut pour chaque type de compte. Pour restreindre davantage l'accès aux fonctionnalités et aux opérations de Macie, vous pouvez utiliser des politiques personnalisées AWS Identity and Access Management (IAM).

Dans le tableau :

- Self indique que le compte ne peut effectuer la tâche pour aucun compte associé.
- Tout indique que le compte peut effectuer la tâche pour un compte associé individuel.
- Tout indique que le compte peut exécuter la tâche et que celle-ci s'applique à tous les comptes associés.

Un tiret (—) indique que le compte ne peut pas effectuer la tâche.

Tâche	À travers AWS Organizations		Sur invitation	
	Administrateur	Membre	Administrateur	Membre
Activez Macie	N'importe quel compte	–	Auto-utilisateur	Auto-utilisateur
Consulter l'inventaire des comptes de l'organisation [1]	Tous	–	Tous	–

Ajouter un compte membre	N'importe quel compte	–	N'importe quel compte	–
Consultez les statistiques et les métadonnées des compartiments S3	Tous	Auto-utilisateur	Tous	Auto-utilisateur
Examiner les conclusions des politiques	Tous	Auto-utilisateur	Tous	Auto-utilisateur
Supprimer (archiver) les résultats des politiques [2]	Tous	–	Tous	–
Publier les conclusions des politiques [3]	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur
Configuration d'un référentiel pour les résultats de découverte de données sensibles [4]	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur
Création et utilisation de listes d'autorisation	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur

Création et utilisation d'identifiants de données personnalisés	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur
Configuration des paramètres de découverte automatique des données sensibles	Tous	–	Tous	–
Activer ou désactiver la découverte automatique des données sensibles	N’importe quel compte	–	N’importe quel compte	–
Passez en revue les statistiques, les données et les résultats de découverte automatique de données sensibles	Tous	–	Tous	–
Création et exécution de tâches de découverte de données sensibles [5]	N’importe quel compte	Auto-utilisateur	N’importe quel compte	Auto-utilisateur

Consultez les détails des tâches de découverte de données sensibles [6]	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur
Examiner les résultats relatifs aux données sensibles [7]	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur
Supprimer (archiver) les résultats de données sensibles [7]	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur
Publier les résultats relatifs aux données sensibles [7]	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur
Configurer Macie pour récupérer des échantill ons de données sensibles pour les résultats	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur
Récupérez des échantillons de données sensibles pour les résultats [8]	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur

Configuration des destinations de publication pour les résultats	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur
Définir la fréquence de publication des résultats	Tous	Auto-utilisateur	Tous	Auto-utilisateur
Créez des exemples de résultats	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur
Vérifiez les quotas de compte et les coûts d'utilisation estimés	Tous	Auto-utilisateur	Tous	Auto-utilisateur
Suspendez Macie [9]	N'importe quel compte	–	N'importe quel compte	Auto-utilisateur
Désactiver Macie [10]	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur	Auto-utilisateur
Supprimer (dissocier) un compte membre	N'importe quel compte	–	N'importe quel compte	–
Dissocier d'un compte administrateur	–	–	–	Auto-utilisateur
Supprimer une association avec un autre compte [11]	N'importe quel compte	–	N'importe quel compte	Auto-utilisateur

1. L'administrateur d'une organisation AWS Organizations peut consulter tous les comptes de l'organisation, y compris les comptes pour lesquels Macie n'est pas activé. L'administrateur d'une organisation basée sur des invitations ne peut consulter que les comptes qu'il ajoute à son inventaire.
2. Seul un administrateur peut supprimer les résultats des politiques. Si un administrateur crée une règle de suppression, Macie l'applique aux conclusions des politiques pour tous les comptes de l'organisation, sauf si la règle est configurée pour exclure des comptes spécifiques. Si un membre crée une règle de suppression, Macie ne l'applique pas aux conclusions de politique relatives au compte du membre.
3. Seul le compte propriétaire d'une ressource affectée peut publier les conclusions des politiques relatives à la ressource AWS Security Hub. Les comptes administrateur et membre publient automatiquement sur Amazon les conclusions relatives aux politiques relatives à une ressource affectée EventBridge.
4. Si un administrateur active la découverte automatique des données sensibles ou configure une tâche pour analyser des objets dans des compartiments S3 détenus par un compte membre, Macie stocke les résultats de la découverte de données sensibles dans le référentiel du compte administrateur.
5. Un membre peut configurer une tâche pour analyser des objets uniquement dans les compartiments S3 détenus par son compte. Un administrateur peut configurer une tâche pour analyser des objets dans des compartiments appartenant à son compte ou à un compte membre. Pour plus d'informations sur la manière dont les quotas sont appliqués et les coûts calculés pour les tâches impliquant plusieurs comptes, consultez. Comprendre comment les coûts d'utilisation estimés sont calculés
6. Seul le compte qui crée une tâche peut accéder aux détails de la tâche. Cela inclut les détails relatifs aux tâches dans l'inventaire des compartiments S3.
7. Seul le compte qui crée une tâche peut accéder aux données sensibles issues de la tâche, les supprimer ou les publier. Seul un administrateur peut accéder aux données sensibles issues de la découverte automatique des données sensibles, les supprimer ou les publier.
8. Si une découverte de données sensibles s'applique à un objet S3 détenu par un compte membre, l'administrateur peut être en mesure de récupérer des échantillons de données sensibles

signalées par la découverte. Cela dépend de la source de la recherche, ainsi que des paramètres de configuration et des ressources du compte administrateur et du compte membre. Pour plus d'informations, consultez la section Options de configuration et exigences relatives à la récupération d'échantillons de données sensibles.

9. Pour qu'un administrateur puisse suspendre Macie pour son propre compte, il doit d'abord dissocier son compte de tous les comptes des membres.

10. Pour qu'un administrateur puisse désactiver Macie pour son propre compte, il doit d'abord dissocier son compte de tous les comptes des membres, puis supprimer les associations entre son compte et tous ces comptes. L'administrateur d'une organisation AWS Organizations peut le faire en utilisant le compte de gestion de l'organisation pour désigner un autre compte en tant que compte administrateur.

    Pour qu'un membre d'une AWS Organizations organisation puisse désactiver Macie, l'administrateur doit d'abord dissocier le compte du membre de son compte administrateur. Dans une organisation basée sur une invitation, le membre peut dissocier son compte de son compte administrateur, puis désactiver Macie.

11. L'administrateur d'une organisation AWS Organizations peut supprimer une association avec un compte membre après avoir dissocié le compte de son compte administrateur. Le compte continue d'apparaître dans l'inventaire des comptes de l'administrateur, mais son statut indique qu'il ne s'agit pas d'un compte de membre. Dans une organisation basée sur une invitation, un administrateur et un membre peuvent supprimer une association avec un autre compte après avoir dissocié leur compte de l'autre compte. L'autre compte cesse alors d'apparaître dans l'inventaire de son compte.

Gestion des comptes Amazon Macie avec AWS Organizations

Si vous avez l'AWS Organizationshabitude de gérer plusieurs comptes de manière centraliséeComptes AWS, vous pouvez intégrer Amazon Macie àAWS Organizations, puis gérer de manière centralisée Macie pour les comptes de votre organisation. Avec cette configuration, un administrateur Macie désigné peut activer et gérer Macie pour un maximum de 10 000 comptes. L'administrateur peut également accéder aux données d'inventaire d'Amazon Simple Storage Service (Amazon S3) et découvrir des données sensibles dans des compartiments S3 détenus par les comptes. Pour plus de détails sur les tâches que l'administrateur peut effectuer, consultezComprendre la relation entre les comptes d'administrateur et de membre d'Amazon Macie.

Pour intégrer Macie àAWS Organizations, vous devez commencer par désigner un compte en tant que compte d'administrateur Macie délégué pour l'organisation. L'administrateur Macie active ensuite Macie pour les autres comptes de l'organisation, ajoute ces comptes en tant que comptes de membres de Macie et configure les paramètres et les ressources de Macie pour les comptes.

> **Tip**
>
> Si vous avez déjà associé un compte administrateur Macie à des comptes de membres à l'aide d'invitations, vous pouvez désigner ce compte comme compte d'administrateur Macie délégué pour votre organisation dans. AWS Organizations Dans ce cas, tous les comptes de membres actuellement associés restent membres et vous pouvez profiter pleinement des avantages de la gestion des comptes en utilisantAWS Organizations. Pour plus d'informations, veuillez consulter Transition depuis une organisation basée sur les invitations.

Les rubriques de cette section expliquent comment intégrer Macie à Macie AWS Organizations et comment administrer et gérer Macie pour les comptes au sein d'une organisation.

Rubriques

- Considérations et recommandations relatives à l'utilisation d'Amazon Macie avec AWS Organizations
- Intégration et configuration d'une organisation dans Amazon Macie
- Révision des comptes Amazon Macie d'une organisation
- Gérer les comptes des membres d'Amazon Macie pour une organisation
- Désignation d'un compte administrateur Amazon Macie différent pour une organisation
- Désactivation de l'intégration d'Amazon Macie avec AWS Organizations

Considérations et recommandations relatives à l'utilisation d'Amazon Macie avec AWS Organizations

Avant d'intégrer Amazon Macie à Macie AWS Organizations et de configurer votre organisation dans Macie, tenez compte des exigences et recommandations suivantes. Assurez-vous également de bien comprendre la relation entre les comptes administrateur et membre de Macie.

Rubriques

- Désignation d'un compte administrateur Macie
- Modifier ou supprimer la désignation d'un compte administrateur Macie
- Ajouter et supprimer des comptes de membres Macie
- Transition depuis une organisation basée sur les invitations

Désignation d'un compte administrateur Macie

Lorsque vous déterminez quel compte doit être le compte administrateur Macie délégué de votre organisation, gardez les points suivants à l'esprit :

- Une organisation ne peut avoir qu'un seul compte administrateur Macie délégué.
- Un compte ne peut pas être un compte administrateur Macie et un compte membre à la fois.
- Seul le compte AWS Organizations de gestion d'une organisation peut désigner le compte administrateur Macie délégué pour l'organisation. Seul le compte de gestion peut ultérieurement modifier ou supprimer cette désignation.
- Le compte AWS Organizations de gestion d'une organisation peut également être le compte administrateur Macie délégué de l'organisation. Cependant, nous ne recommandons pas cette configuration sur la base des meilleures pratiques de AWS sécurité et du principe du moindre privilège. Les utilisateurs qui ont accès au compte de gestion à des fins de facturation sont susceptibles d'être différents des utilisateurs qui ont besoin d'accéder à Macie pour des raisons de sécurité des informations.

  Si vous préférez cette configuration, vous devez activer Macie pour le compte de gestion de l'organisation dans au moins un compte Région AWS avant de le désigner comme compte administrateur Macie délégué. Sinon, le compte ne sera pas en mesure d'accéder aux paramètres et aux ressources Macie pour les comptes des membres et de les gérer.
- Contrairement AWS Organizationsà Macie est un service régional. Cela signifie que la désignation d'un compte administrateur Macie est une désignation régionale. Cela signifie également que les associations entre les comptes administrateur et membre de Macie sont régionales. Par exemple, si le compte de gestion désigne un compte administrateur Macie dans la région USA Est (Virginie du Nord), l'administrateur Macie peut gérer Macie pour les comptes des membres uniquement dans cette région.

  Pour gérer de manière centralisée plusieurs comptes Macie Régions AWS, le compte de gestion doit se connecter à chaque région dans laquelle l'organisation utilise actuellement ou utilisera Macie, puis désigner le compte administrateur Macie dans chacune de ces régions.

L'administrateur Macie peut ensuite configurer l'organisation dans chacune de ces régions. Pour obtenir la liste des régions dans lesquelles Macie est actuellement disponible, consultez la section Points de terminaison et quotas Amazon Macie dans le. Références générales AWS

- Un compte ne peut être associé qu'à un seul compte administrateur Macie à la fois. Si votre organisation utilise Macie dans plusieurs régions, le compte administrateur Macie désigné doit être le même dans toutes ces régions. Toutefois, le compte de gestion de votre organisation doit désigner le compte administrateur séparément dans chaque région.
- Un compte ne peut être le compte d'administrateur Macie délégué que pour une seule organisation à la fois. Si vous gérez plusieurs organisations dans AWS Organizations, vous devez désigner un compte administrateur Macie différent pour chaque organisation. Cela est dû à une AWS Organizations exigence : un compte ne peut être membre que d'une seule organisation à la fois.

Si l'administrateur Macie Compte AWS est suspendu, isolé ou fermé, tous les comptes de membre Macie associés sont automatiquement supprimés en tant que comptes de membre Macie, mais Macie continue d'être activé pour ces comptes. Si la découverte automatique des données sensibles a été activée pour un ou plusieurs comptes membres, elle est désactivée pour les comptes. Cela désactive également l'accès aux données statistiques, aux données d'inventaire et aux autres informations produites et fournies directement par Macie lors de la découverte automatique des comptes. Pour rétablir l'accès à ces données, les mesures suivantes doivent être prises dans les 30 jours :

1. Celui de l'administrateur Macie Compte AWS est restauré.
2. Le compte AWS Organizations de gestion désigne à nouveau le compte en tant que compte administrateur Macie.
3. L'administrateur Macie configure l'organisation et active à nouveau la découverte automatique des comptes appropriés.

Au bout de 30 jours, Macie supprime définitivement les données qu'elle a précédemment produites et directement fournies tout en effectuant une découverte automatique pour les comptes concernés.

Modifier ou supprimer la désignation d'un compte administrateur Macie

Seul le compte AWS Organizations de gestion d'une organisation peut modifier ou supprimer la désignation d'un compte administrateur Macie délégué pour l'organisation.

Si le compte de gestion modifie ou supprime la désignation :

- Tous les comptes de membre associés sont supprimés en tant que comptes de membres Macie, mais Macie continue d'être activé pour les comptes. Les comptes deviennent des comptes Macie autonomes. Pour suspendre ou arrêter d'utiliser Macie, l'utilisateur d'un compte membre doit suspendre (suspendre) ou désactiver (arrêter) Macie pour le compte.
- La découverte automatique des données sensibles est désactivée pour chaque compte pour lequel elle a été activée. Cela désactive également l'accès aux données statistiques, aux données d'inventaire et aux autres informations produites et fournies directement par Macie lors de la découverte automatique de chaque compte. Pour rétablir l'accès à ces données, le compte de gestion doit à nouveau désigner le même compte administrateur Macie dans les 30 jours. En outre, l'administrateur Macie doit reconfigurer l'organisation et réactiver la découverte automatique pour chaque compte dans un délai de 30 jours. Après 30 jours, les données expirent et Macie les supprime définitivement.

Ajouter et supprimer des comptes de membres Macie

Lorsque vous ajoutez, supprimez ou gérez des comptes de membres pour votre organisation, gardez les points suivants à l'esprit :

- Un compte administrateur Macie ne peut pas être associé à plus de 10 000 comptes de membres Macie actifs (activés) dans chacun d'eux. Région AWS Si votre organisation dépasse ce quota, l'administrateur Macie ne pourra pas ajouter de comptes membres tant qu'il n'aura pas supprimé le nombre nécessaire de comptes membres existants dans la région. Lorsqu'une organisation atteint ce quota, nous en informons l'administrateur Macie en créant AWS Health des CloudWatch événements Amazon pour son compte. Nous envoyons également un e-mail à l'adresse associée à leur compte.

  Si vous êtes l'administrateur Macie d'une organisation, vous pouvez déterminer le nombre de comptes de membres actifs actuellement associés à votre compte en utilisant la page Comptes de la console Amazon Macie ou en utilisant ListMembersl'API Amazon Macie. Pour plus d'informations, consultez Révision des comptes Amazon Macie d'une organisation.
- Un compte ne peut être associé qu'à un seul compte administrateur Macie à la fois. Cela signifie qu'un compte ne peut pas accepter une invitation Macie provenant d'un autre compte s'il est déjà associé au compte administrateur Macie d'une organisation dans. AWS Organizations

  De même, si un compte a déjà accepté une invitation, l'administrateur Macie d'une organisation ne AWS Organizations peut pas ajouter le compte en tant que compte membre Macie. Le compte doit d'abord se dissocier de son compte administrateur actuel, basé sur des invitations.

- Pour ajouter le compte AWS Organizations de gestion en tant que compte membre Macie, un utilisateur du compte de gestion doit d'abord activer Macie pour le compte. L'administrateur Macie n'est pas autorisé à activer Macie pour le compte de gestion.
- Si l'administrateur Macie supprime le compte d'un membre Macie :
  - Macie continue d'être activé pour le compte. Le compte devient un compte Macie autonome. Pour suspendre ou arrêter d'utiliser Macie, un utilisateur du compte doit suspendre (pause) ou désactiver (arrêter) Macie pour le compte.
  - La découverte automatique des données sensibles est désactivée pour le compte, si elle a été activée. Cela désactive également l'accès aux données statistiques, aux données d'inventaire et aux autres informations produites et fournies directement par Macie lors de la découverte automatique du compte.
- Un compte membre ne peut pas être dissocié de son compte administrateur Macie. Seul l'administrateur de Macie peut supprimer un compte en tant que compte de membre de Macie.

Transition depuis une organisation basée sur les invitations

Si vous avez déjà associé un compte administrateur Macie à des comptes de membres en utilisant des invitations d'adhésion Macie, nous vous recommandons de désigner ce compte comme compte administrateur Macie délégué pour votre organisation dans. AWS Organizations Cela simplifie la transition depuis une organisation basée sur les invitations.

Dans ce cas, tous les comptes de membres actuellement associés restent membres. Si un compte membre fait partie de votre organisation dans AWS Organizations, l'association du compte passe automatiquement de By invitation à Via AWS Organizations in Macie. Si le compte d'un membre ne fait pas partie de votre organisation dans AWS Organizations, l'association du compte continue d'être sur invitation. Dans les deux cas, les comptes continuent d'être associés au compte administrateur Macie délégué en tant que comptes de membre.

Nous recommandons cette approche car un compte ne peut pas être associé à plusieurs comptes d'administrateur Macie à la fois. Si vous désignez un autre compte comme compte administrateur Macie pour votre organisation dans AWS Organizations, l'administrateur désigné ne pourra pas gérer les comptes déjà associés à un autre compte administrateur Macie sur invitation. Chaque compte membre doit d'abord se dissocier de son compte administrateur actuel, basé sur des invitations. L'administrateur Macie de votre organisation AWS Organizations peut ensuite ajouter le compte en tant que compte membre Macie et commencer à gérer le compte.

Après avoir intégré Macie à Macie AWS Organizations et configuré votre organisation dans Macie, vous pouvez éventuellement désigner un compte administrateur Macie différent pour l'organisation. Vous pouvez également continuer à utiliser des invitations pour associer et gérer des comptes de membres qui ne font pas partie de votre organisation AWS Organizations.

Intégration et configuration d'une organisation dans Amazon Macie

Pour commencer à utiliser Amazon Macie avec AWS Organizations, le compte de AWS Organizations gestion de l'organisation désigne un compte en tant que compte administrateur Macie délégué pour l'organisation. Cela permet à Macie de devenir un service de confiance dans AWS Organizations. Il active également Macie en cours Région AWS pour le compte administrateur désigné, et il permet au compte administrateur désigné d'activer et de gérer Macie pour les autres comptes de l'organisation dans cette région. Pour plus d'informations sur la manière dont ces autorisations sont accordées, voir Utilisation AWS Organizations avec d'autres personnes Services AWS dans le Guide de AWS Organizations l'utilisateur.

L'administrateur délégué de Macie configure ensuite l'organisation dans Macie, principalement en ajoutant les comptes de l'organisation en tant que comptes de membres de Macie dans la région. L'administrateur peut ensuite accéder à certains paramètres, données et ressources Macie pour ces comptes dans cette région. Ils peuvent également effectuer une découverte automatique des données sensibles et exécuter des tâches de découverte de données sensibles pour détecter les données sensibles dans les compartiments Amazon Simple Storage Service (Amazon S3) détenus par les comptes.

Cette rubrique explique comment désigner un administrateur Macie délégué pour une organisation et comment ajouter les comptes de l'organisation en tant que comptes de membres Macie. Avant d'effectuer ces tâches, assurez-vous de bien comprendre la relation entre les comptes administrateur et membre. Il est également conseillé de passer en revue les considérations et les recommandations relatives à l'utilisation de Macie avec AWS Organizations.

Tâches

- Étape 1 : Vérifier vos autorisations
- Étape 2 : Désigner le compte administrateur Macie délégué pour l'organisation
- Étape 3 : activer et ajouter automatiquement de nouveaux comptes d'organisation en tant que comptes membres de Macie
- Étape 4 : activer et ajouter des comptes d'organisation existants en tant que comptes membres Macie

Pour intégrer et configurer l'organisation dans plusieurs régions, le compte AWS Organizations de gestion et l'administrateur Macie délégué répètent ces étapes dans chaque région supplémentaire.

Étape 1 : Vérifier vos autorisations

Avant de désigner le compte administrateur Macie délégué pour votre organisation, vérifiez que vous (en tant qu'utilisateur du compte de AWS Organizations gestion) êtes autorisé à effectuer l'action Macie suivante : `macie2:EnableOrganizationAdminAccount` Cette action vous permet de désigner le compte administrateur Macie délégué pour votre organisation à l'aide de Macie.

Vérifiez également que vous êtes autorisé à effectuer les AWS Organizations actions suivantes :

- `organizations:DescribeOrganization`
- `organizations:EnableAWSServiceAccess`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:RegisterDelegatedAdministrator`

Ces actions vous permettent de : récupérer des informations sur votre organisation ; intégrer Macie à AWS Organizations ; récupérer des informations à propos desquelles Services AWS vous avez intégré AWS Organizations ; et désigner un compte administrateur Macie délégué pour votre organisation.

Pour accorder ces autorisations, incluez la déclaration suivante dans une politique AWS Identity and Access Management (IAM) pour votre compte :

```
{
   "Sid": "Grant permissions to designate a delegated Macie administrator",
   "Effect": "Allow",
   "Action": [
      "macie2:EnableOrganizationAdminAccount",
      "organizations:DescribeOrganization",
      "organizations:EnableAWSServiceAccess",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:RegisterDelegatedAdministrator"
   ],
   "Resource": "*"
}
```

Si vous souhaitez désigner votre compte AWS Organizations de gestion comme compte administrateur Macie délégué pour l'organisation, votre compte doit également être autorisé à

effectuer l'action IAM suivante :. `CreateServiceLinkedRole` Cette action vous permet d'activer Macie pour le compte de gestion. Toutefois, conformément aux meilleures pratiques en matière de AWS sécurité et au principe du moindre privilège, nous vous déconseillons de le faire.

Si vous décidez d'accorder cette autorisation, ajoutez la déclaration suivante à la politique IAM de votre compte AWS Organizations de gestion :

```
{
   "Sid": "Grant permissions to enable Macie",
   "Effect": "Allow",
   "Action": [
      "iam:CreateServiceLinkedRole"
   ],
   "Resource": "arn:aws:iam::111122223333:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
   "Condition": {
      "StringLike": {
         "iam:AWSServiceName": "macie.amazonaws.com"
      }
   }
}
```

Dans le relevé, remplacez *111122223333* par le numéro de compte du compte de gestion.

Si vous souhaitez administrer Macie dans le cadre d'un opt-in Région AWS (région désactivée par défaut), mettez également à jour la valeur du principal de service Macie dans l'`Resource`élément et la condition. `iam:AWSServiceName` La valeur doit spécifier le code de région pour la région. Par exemple, pour administrer Macie dans la région du Moyen-Orient (Bahreïn), dont le code de région est me-south-1, procédez comme suit :

- Dans l'`Resource`élément, remplacez

  `arn:aws:iam::111122223333:role/aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`

  avec

  `arn:aws:iam::111122223333:role/aws-service-role/macie.me-south-1.amazonaws.com/AWSServiceRoleForAmazonMacie`

Où *111122223333* indique l'identifiant du compte de gestion et me-south-1 indique le code de région de *la* région.

- Dans la `iam:AWSServiceName` condition, remplacez `macie.amazonaws.com` par`macie.me-south-1.amazonaws.com`, où *me-south-1* indique le code de région pour la région.

Pour obtenir la liste des régions dans lesquelles Macie est actuellement disponible et le code régional de chacune d'entre elles, consultez la section Points de terminaison et quotas Amazon Macie dans le. Références générales AWS Pour plus d'informations sur les régions d'adhésion, voir Spécifier les régions que Régions AWS votre compte peut utiliser dans le Guide de AWS Account Management référence.

Étape 2 : Désigner le compte administrateur Macie délégué pour l'organisation

Après avoir vérifié vos autorisations, vous (en tant qu'utilisateur du compte de AWS Organizations gestion) pouvez désigner le compte administrateur Macie délégué pour votre organisation.

Pour désigner le compte administrateur Macie délégué pour une organisation

Pour désigner le compte administrateur Macie délégué pour votre organisation, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie. Seul un utilisateur du compte AWS Organizations de gestion peut effectuer cette tâche.

Console

Suivez ces étapes pour désigner le compte administrateur Macie délégué à l'aide de la console Amazon Macie.

Pour désigner le compte administrateur Macie délégué

1. Connectez-vous à l' AWS Management Console aide de votre compte AWS Organizations de gestion.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez désigner le compte d'administrateur Macie délégué pour votre organisation.
3. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
4. Procédez de l'une des manières suivantes, selon que Macie est activé ou non pour votre compte de gestion dans la région actuelle :

- Si Macie n'est pas activé, choisissez Commencer sur la page d'accueil.
- Si Macie est activé, choisissez Paramètres dans le volet de navigation.

5. Sous Administrateur délégué, entrez l'identifiant de compte à 12 chiffres pour le compte Compte AWS que vous souhaitez désigner comme compte administrateur Macie.
6. Choisisssez Delegate (Déléguer).

Répétez les étapes précédentes dans chaque région supplémentaire dans laquelle vous souhaitez intégrer votre organisation à Macie. Vous devez désigner le même compte administrateur Macie dans chacune de ces régions.

API

Pour désigner le compte administrateur Macie délégué par programmation, utilisez le EnableOrganizationAdminAccountfonctionnement de l'API Amazon Macie. Pour désigner le compte dans plusieurs régions, soumettez la désignation de chaque région dans laquelle vous souhaitez intégrer votre organisation à Macie. Vous devez désigner le même compte administrateur Macie dans chacune de ces régions.

Lorsque vous soumettez la désignation, utilisez le `adminAccountId` paramètre requis pour spécifier l'identifiant de compte à 12 chiffres Compte AWS à désigner comme compte administrateur Macie pour l'organisation. Assurez-vous également de spécifier la région à laquelle la désignation s'applique.

Pour désigner le compte administrateur Macie à l'aide de AWS Command Line Interface (AWS CLI), exécutez la enable-organization-admin-accountcommande. Pour le `admin-account-id` paramètre, spécifiez l'identifiant de compte à 12 chiffres Compte AWS à désigner. Utilisez le `region` paramètre pour spécifier la région à laquelle la désignation s'applique. Par exemple :

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-account-id 111122223333
```

Où *`us-east-1`* est la région à laquelle s'applique la désignation (la région USA Est (Virginie du Nord)) *`et`* 111122223333 est le numéro de compte du compte à désigner.

Après avoir désigné le compte administrateur Macie pour votre organisation, l'administrateur Macie peut commencer à configurer l'organisation dans Macie.

Étape 3 : activer et ajouter automatiquement de nouveaux comptes d'organisation en tant que comptes membres de Macie

Par défaut, Macie n'est pas automatiquement activé pour les nouveaux comptes lorsque ceux-ci sont ajoutés à votre organisation dans AWS Organizations. De plus, les comptes ne sont pas automatiquement ajoutés en tant que comptes membres de Macie. Les comptes apparaissent dans l'inventaire des comptes de l'administrateur Macie. Cependant, Macie n'est pas nécessairement activé pour les comptes et l'administrateur Macie ne peut pas nécessairement accéder aux paramètres, aux données et aux ressources de Macie pour les comptes.

Si vous êtes l'administrateur Macie délégué de l'organisation, vous pouvez modifier ce paramètre de configuration. Vous pouvez activer l'activation automatique pour votre organisation. Dans ce cas, Macie est automatiquement activé pour les nouveaux comptes lorsque les comptes sont ajoutés à votre organisation dans AWS Organizations, et les comptes sont automatiquement associés à votre compte administrateur Macie en tant que comptes de membre. L'activation de ce paramètre n'affecte pas les comptes existants de votre organisation. Pour activer et gérer Macie pour les comptes existants, vous devez ajouter manuellement les comptes en tant que comptes membres Macie. L'étape suivante explique comment procéder.

> **Remarques**
>
> Si vous activez l'activation automatique, notez les exceptions suivantes :
>
> - Si un nouveau compte est déjà associé à un autre compte administrateur Macie, Macie n'ajoute pas automatiquement le compte en tant que compte membre de votre organisation.
>
> Le compte doit être dissocié de son compte administrateur Macie actuel avant de pouvoir faire partie de votre organisation dans Macie. Vous pouvez ensuite ajouter le compte manuellement. Pour identifier les comptes dans lesquels c'est le cas, vous pouvez consulter l'inventaire des comptes de votre organisation.
> - Si votre organisation atteint le quota de 10 000 comptes membres Macie par an Région AWS, Macie désactive automatiquement ce paramètre dans la région.
>
> Dans ce cas, nous vous en informerons en créant AWS Health des CloudWatch événements Amazon pour votre compte administrateur Macie. Nous envoyons également un e-mail à l'adresse associée à ce compte. Si le nombre total de comptes diminue par la suite à moins de 10 000 comptes, Macie réactive automatiquement le paramètre.

Pour activer et ajouter automatiquement de nouveaux comptes d'organisation en tant que comptes membres de Macie

Pour activer et ajouter automatiquement de nouveaux comptes en tant que comptes membres Macie, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie. Seul l'administrateur Macie délégué de l'organisation peut effectuer cette tâche.

Console

Pour effectuer cette tâche à l'aide de la console, vous devez être autorisé à effectuer l' AWS Organizations action suivante : `organizations:ListAccounts` Cette action vous permet de récupérer et d'afficher des informations sur les comptes de votre organisation. Si vous disposez de ces autorisations, suivez ces étapes pour activer et ajouter automatiquement de nouveaux comptes d'organisation en tant que comptes membres de Macie.

Pour activer et ajouter automatiquement de nouveaux comptes d'organisation

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez activer et ajouter automatiquement de nouveaux comptes en tant que comptes membres Macie.
3. Dans le panneau de navigation, choisissez Accounts (Comptes).
4. Sur la page Comptes, dans la section Nouveaux comptes, choisissez Modifier.
5. Dans la boîte de dialogue Modifier les paramètres pour les nouveaux comptes, sélectionnez Activer Macie.

   Pour activer également la découverte automatique des données sensibles pour les nouveaux comptes membres, sélectionnez Activer la découverte automatique des données sensibles. Si vous activez cette fonctionnalité pour un compte, Macie sélectionne en permanence des échantillons d'objets dans les compartiments S3 du compte et analyse les objets pour déterminer s'ils contiennent des données sensibles. Pour plus d'informations, consultez Réalisation de la découverte automatisée des données sensibles.
6. Choisissez Enregistrer.

Répétez les étapes précédentes dans chaque région supplémentaire dans laquelle vous souhaitez configurer votre organisation dans Macie.

Pour modifier ultérieurement ces paramètres, répétez les étapes précédentes et décochez la case correspondant à chaque paramètre.

API

Pour activer et ajouter automatiquement de nouveaux comptes membres Macie par programmation, utilisez l'API UpdateOrganizationConfigurationAmazon Macie. Lorsque vous soumettez votre demande, définissez la valeur du `autoEnable` paramètre sur`true`. (La valeur par défaut est `false`.) Assurez-vous également de spécifier la région à laquelle s'applique votre demande. Pour activer et ajouter automatiquement de nouveaux comptes dans des régions supplémentaires, soumettez la demande pour chaque région supplémentaire.

Si vous utilisez le AWS CLI pour envoyer la demande, exécutez la update-organization-configurationcommande et spécifiez le `auto-enable` paramètre pour activer et ajouter de nouveaux comptes automatiquement. Par exemple :

```
$ aws macie2 update-organization-configuration --region us-east-1 --auto-enable
```

Où *`us-east-1`* est la région dans laquelle il est possible d'activer et d'ajouter automatiquement de nouveaux comptes, la région USA Est (Virginie du Nord).

Pour modifier ultérieurement ce paramètre et arrêter d'activer et d'ajouter automatiquement de nouveaux comptes, réexécutez la même commande et utilisez le `no-auto-enable` paramètre, au lieu du `auto-enable` paramètre, dans chaque région applicable.

Vous pouvez également activer la découverte automatique des données sensibles pour les nouveaux comptes membres. Si vous activez cette fonctionnalité pour un compte, Macie sélectionne en permanence des échantillons d'objets dans les compartiments S3 du compte et analyse les objets pour déterminer s'ils contiennent des données sensibles. Pour plus d'informations, consultez Réalisation de la découverte automatisée des données sensibles. Pour activer automatiquement cette fonctionnalité pour les comptes des membres, utilisez l'UpdateAutomatedDiscoveryConfigurationopération ou, si vous utilisez le AWS CLI, exécutez la update-automated-discovery-configurationcommande.

Étape 4 : activer et ajouter des comptes d'organisation existants en tant que comptes membres Macie

Lorsque vous intégrez Macie à Macie AWS Organizations, Macie n'est pas automatiquement activé pour tous les comptes existants de votre organisation. De plus, les comptes ne sont pas

automatiquement associés au compte administrateur Macie délégué en tant que comptes de membre Macie. Par conséquent, la dernière étape de l'intégration et de la configuration de votre organisation dans Macie consiste à ajouter des comptes d'organisation existants en tant que comptes membres de Macie. Lorsque vous ajoutez un compte existant en tant que compte membre Macie, Macie est automatiquement activé pour le compte et vous (en tant qu'administrateur Macie délégué) avez accès à certains paramètres, données et ressources Macie du compte.

Notez que vous ne pouvez pas ajouter un compte actuellement associé à un autre compte administrateur Macie. Pour ajouter le compte, contactez le propriétaire du compte pour dissocier d'abord le compte de son compte administrateur actuel. De plus, vous ne pouvez pas ajouter de compte existant si Macie est actuellement suspendu pour ce compte. Le titulaire du compte doit d'abord réactiver Macie pour le compte. Enfin, si vous souhaitez ajouter le compte de AWS Organizations gestion en tant que compte membre, un utilisateur de ce compte doit d'abord activer Macie pour le compte.

Pour activer et ajouter des comptes d'organisation existants en tant que comptes membres de Macie

Pour activer et ajouter des comptes d'organisation existants en tant que comptes membres de Macie, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie. Seul l'administrateur Macie délégué de l'organisation peut effectuer cette tâche.

Console

Pour effectuer cette tâche à l'aide de la console, vous devez être autorisé à effectuer l' AWS Organizations action suivante : `organizations:ListAccounts` Cette action vous permet de récupérer et d'afficher des informations sur les comptes de votre organisation. Si vous disposez de ces autorisations, procédez comme suit pour activer et ajouter des comptes existants en tant que comptes membres Macie.

Pour activer et ajouter des comptes d'organisation existants

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez activer et ajouter des comptes existants en tant que comptes membres Macie.
3. Dans le panneau de navigation, choisissez Accounts (Comptes).

La page Comptes s'ouvre et affiche un tableau des comptes associés à votre compte Macie. Si un compte fait partie de votre organisation dans AWS Organizations, son type est Via AWS Organizations. Si un compte est déjà un compte membre de Macie, son statut est Activé.

4. Dans le tableau Comptes, cochez la case correspondant à chaque compte que vous souhaitez ajouter en tant que compte membre Macie.
5. Dans le menu Actions, choisissez Ajouter un membre.
6. Confirmez que vous souhaitez ajouter les comptes sélectionnés en tant que comptes membres.

Une fois que vous avez confirmé l'ajout des comptes sélectionnés, le statut des comptes passe à Activation en cours, puis à Activé. Après avoir ajouté un compte membre, vous pouvez également activer la découverte automatique des données sensibles pour le compte : dans le tableau Comptes, cochez la case correspondant à chaque compte, puis choisissez Activer la découverte automatique des données sensibles dans le menu Actions. Si vous activez cette fonctionnalité pour un compte, Macie sélectionne en permanence des échantillons d'objets dans les compartiments S3 du compte et analyse les objets pour déterminer s'ils contiennent des données sensibles. Pour plus d'informations, consultez Réalisation de la découverte automatisée des données sensibles.

Répétez les étapes précédentes dans chaque région supplémentaire dans laquelle vous souhaitez configurer votre organisation dans Macie.

API

Pour activer et ajouter par programmation un ou plusieurs comptes existants en tant que comptes membres Macie, utilisez le CreateMemberfonctionnement de l'API Amazon Macie. Lorsque vous soumettez votre demande, utilisez les paramètres pris en charge pour spécifier l'identifiant de compte à 12 chiffres et l'adresse e-mail de chacun Compte AWS à activer et à ajouter. Spécifiez également la région à laquelle s'applique la demande. Pour activer et ajouter des comptes existants dans d'autres régions, soumettez la demande pour chaque région supplémentaire.

Pour récupérer l'identifiant de compte et l'adresse e-mail d'un Compte AWS utilisateur à activer et à ajouter, vous pouvez éventuellement utiliser le ListMembersfonctionnement de l'API Amazon Macie. Cette opération fournit des détails sur les comptes associés à votre compte Macie, y compris les comptes qui ne sont pas des comptes de membres de Macie. Si la valeur de la `relationshipStatus` propriété d'un compte ne l'est pas`Enabled`, il ne s'agit pas d'un compte de membre Macie.

Pour activer et ajouter un ou plusieurs comptes existants à l'aide de AWS CLI, exécutez la commande create-member. Utilisez le `region` paramètre pour spécifier la région dans laquelle vous souhaitez activer et ajouter les comptes. Utilisez les `account` paramètres pour spécifier l'ID de compte et l'adresse e-mail de chacun Compte AWS à ajouter. Par exemple :

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"123456789012\",\"email\":\"janedoe@example.com\"}
```

Où us-east-1 est la région dans laquelle activer et ajouter le compte en tant que compte de membre Macie (région USA Est (Virginie du Nord)), et les paramètres spécifient l'ID du compte (123456789012) et account l'adresse e-mail (janedoe@example.com) du compte.

Si votre demande aboutit, le statut (`relationshipStatus`) du compte spécifié est reporté `Enabled` à l'inventaire de votre compte.

Pour activer également la découverte automatique des données sensibles pour un ou plusieurs comptes, utilisez l'BatchUpdateAutomatedDiscoveryAccountsopération ou, si vous utilisez le AWS CLI, exécutez la commande batch-update-automated-discovery-accounts. Si vous activez cette fonctionnalité pour un compte, Macie sélectionne en permanence des échantillons d'objets dans les compartiments S3 du compte et analyse les objets pour déterminer s'ils contiennent des données sensibles. Pour plus d'informations, voir Réalisation de la découverte automatisée des données sensibles.

Révision des comptes Amazon Macie d'une organisation

Une fois qu'une AWS Organizations organisation est intégrée et configurée dans Amazon Macie, l'administrateur Macie délégué peut accéder à un inventaire des comptes de l'organisation dans Macie. En tant qu'administrateur Macie d'une organisation, vous pouvez utiliser cet inventaire pour consulter les statistiques et les détails des comptes Macie de votre organisation dans un. Région AWS Vous pouvez également l'utiliser pour effectuer certaines tâches de gestion des comptes.

Pour consulter les comptes Macie d'une organisation

Pour consulter les comptes de votre organisation, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie. Si vous préférez utiliser la console, vous devez être autorisé à effectuer l' AWS Organizations action suivante : `organizations:ListAccounts` Cette action vous permet de récupérer et d'afficher des informations sur les comptes qui font partie de votre organisation dans AWS Organizations.

Console

Suivez ces étapes pour consulter les comptes Macie de votre organisation à l'aide de la console Amazon Macie.

Pour consulter les comptes de votre organisation

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez consulter les comptes de votre organisation.
3. Dans le panneau de navigation, choisissez Accounts (Comptes).

La page Comptes s'ouvre et affiche des statistiques agrégées ainsi qu'un tableau des comptes actuellement Région AWS associés à votre compte Macie.

En haut de la page Comptes, vous trouverez les statistiques agrégées suivantes.

Via AWS Organizations

Active indique le nombre total de comptes associés à votre compte par le biais de comptes membres Macie de votre organisation AWS Organizations et qui sont actuellement membres de Macie. Macie est activé pour ces comptes et vous êtes l'administrateur Macie des comptes.

All indique le nombre total de comptes associés à votre compte via AWS Organizations, y compris les comptes qui ne sont pas actuellement des comptes membres de Macie.

Sur invitation

Active indique le nombre total de comptes associés à votre compte sur invitation de Macie et qui sont actuellement des comptes membres de Macie. Ces comptes ne sont pas associés à votre compte par le biais de AWS Organizations. Macie est activé pour les comptes et vous êtes l'administrateur Macie des comptes car ils ont accepté une invitation d'adhésion à Macie de votre part.

All indique le nombre total de comptes associés à votre compte par invitation Macie, y compris les comptes qui n'ont pas répondu à une invitation de votre part.

Actif/Tout

Active indique le nombre total de comptes actuellement membres de Macie pour votre compte, via AWS Organizations ou sur invitation de Macie. Macie est activé pour ces comptes et vous êtes l'administrateur Macie des comptes.

All indique le nombre total de comptes associés à votre compte, via AWS Organizations ou sur invitation de Macie. Cela inclut les comptes qui font partie de votre organisation AWS Organizations et qui ne sont pas actuellement des comptes membres de Macie, ainsi que les comptes qui n'ont pas répondu à une invitation d'adhésion à Macie de votre part.

Dans le tableau, vous trouverez des informations sur chaque compte de la région actuelle. Le tableau inclut tous les comptes associés à votre compte Macie, via AWS Organizations ou sur invitation de Macie.

ID de compte

L'identifiant du compte et l'adresse e-mail du Compte AWS.

Nom

Le nom du compte pour Compte AWS. Cette valeur est généralement N/A pour les comptes associés à votre compte sur invitation de Macie.

Type

Comment le compte est associé à votre compte, via AWS Organizations ou sur invitation de Macie.

Statut

État de la relation entre votre compte et le compte. Pour un compte dans une AWS Organizations organisation (Type is Via AWS Organizations), les valeurs possibles sont les suivantes :

- Compte suspendu — Le compte Compte AWS est suspendu.
- Créé/Activation — Macie traite une demande d'activation et d'ajout du compte en tant que compte membre Macie.
- Activé — Le compte est un compte de membre Macie. Macie est activé pour le compte et vous êtes l'administrateur Macie du compte.
- Non membre : le compte fait partie de votre organisation, AWS Organizations mais il ne s'agit pas d'un compte de membre Macie.
- Suspendu (suspendu) — Le compte est un compte de membre de Macie, mais Macie est actuellement suspendu pour le compte.
- Région désactivée — Le compte fait partie de votre organisation AWS Organizations mais la région actuelle est désactivée pour le Compte AWS.

- Supprimé (dissocié) — Le compte était auparavant un compte de membre Macie, mais il a ensuite été supprimé en tant que compte de membre. Vous avez dissocié le compte de votre compte administrateur Macie. Macie continue d'être activé pour le compte.

Dernière mise à jour du statut

Lorsque vous ou le compte associé avez récemment effectué une action qui a eu une incidence sur la relation entre vos comptes.

Découverte automatisée des données sensibles

Si la découverte automatique des données sensibles est actuellement activée ou désactivée pour le compte.

Pour trier le tableau en fonction d'un champ spécifique, choisissez l'en-tête de colonne du champ. Pour modifier l'ordre de tri, choisissez à nouveau l'en-tête de colonne. Pour filtrer le tableau, placez votre curseur dans la zone de filtre, puis ajoutez une condition de filtre pour un champ. Pour affiner davantage les résultats, ajoutez des conditions de filtre pour des champs supplémentaires.

API

Pour consulter les comptes de votre organisation par programmation, utilisez l'ListMembersAPI Amazon Macie et spécifiez la région à laquelle s'applique votre demande. Pour consulter les comptes dans d'autres régions, soumettez votre demande dans chaque région supplémentaire.

Lorsque vous soumettez votre demande, utilisez le `onlyAssociated` paramètre pour spécifier les comptes à inclure dans la réponse. Par défaut, Macie renvoie uniquement les informations relatives aux comptes membres de Macie dans la région spécifiée, via AWS Organizations ou sur invitation de Macie. Pour récupérer ces informations pour tous les comptes associés à votre compte Macie, y compris les comptes qui ne sont pas des comptes membres, incluez le `onlyAssociated` paramètre dans votre demande et définissez la valeur du paramètre sur`false`.

Pour consulter les comptes de votre organisation à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande list-members. Pour le `only-associated` paramètre, spécifiez si vous souhaitez inclure tous les comptes associés ou uniquement les comptes membres de Macie. Pour inclure uniquement les comptes des membres, omettez ce paramètre ou définissez la valeur du paramètre sur`true`. Pour inclure tous les comptes, définissez cette valeur sur`false`. Par exemple :

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

Où *us-east-1* est la région à laquelle s'applique la demande, la région USA Est (Virginie du Nord).

Si votre demande aboutit, Macie renvoie un `members` tableau. Le tableau contient un `member` objet pour chaque compte qui répond aux critères spécifiés dans la demande. Dans cet objet, le `relationshipStatus` champ indique l'état actuel de la relation entre votre compte et l'autre compte dans la région spécifiée. Pour un compte dans une AWS Organizations organisation, les valeurs possibles sont les suivantes :

- `AccountSuspended`— Le Compte AWS est suspendu.
- `Created`— Macie traite une demande d'activation et d'ajout du compte en tant que compte de membre Macie.
- `Enabled`— Le compte est un compte de membre Macie. Macie est activé pour le compte et vous êtes l'administrateur Macie du compte.
- `Paused`— Le compte est un compte de membre de Macie, mais Macie est actuellement suspendu (suspendu) pour le compte.
- `RegionDisabled`— Le compte fait partie de votre organisation AWS Organizations , mais la région actuelle est désactivée pour le Compte AWS.
- `Removed`— Le compte était auparavant un compte de membre Macie, mais il a ensuite été supprimé en tant que compte de membre. Vous avez dissocié le compte de votre compte administrateur Macie. Macie continue d'être activé pour le compte.

Pour plus d'informations sur les autres champs de l'`member`objet, consultez la section Membres du manuel Amazon Macie API Reference.

Gérer les comptes des membres d'Amazon Macie pour une organisation

Une fois qu'une AWS Organizations organisation est intégrée et configurée dans Amazon Macie, l'administrateur Macie délégué de l'organisation peut accéder à certains paramètres, données et ressources Macie pour les comptes des membres.

En tant qu'administrateur Macie d'une organisation, vous pouvez effectuer de manière centralisée certaines tâches de gestion et d'administration des comptes dans Macie. Par exemple :

- Ajouter et supprimer des comptes de membres Macie
- Gérez le statut de Macie pour les comptes individuels, par exemple en activant ou en suspendant Macie pour un compte
- Surveillez les quotas Macie et les coûts d'utilisation estimés pour les comptes individuels et pour l'ensemble de l'organisation

Vous pouvez également consulter les données d'inventaire d'Amazon Simple Storage Service (Amazon S3) et les conclusions relatives aux politiques relatives aux comptes membres de Macie. Et vous pouvez découvrir des données sensibles dans les compartiments S3 détenus par les comptes. Pour une liste détaillée des tâches que vous pouvez effectuer, consultezComprendre la relation entre les comptes d'administrateur et de membre d'Amazon Macie.

Par défaut, Macie vous donne une visibilité sur les données et les ressources pertinentes pour tous les comptes membres Macie de votre organisation. Vous pouvez également effectuer une analyse descendante pour consulter les données et les ressources des comptes individuels. Par exemple, si vous utilisez le tableau de bord récapitulatif pour évaluer le niveau de sécurité de votre organisation sur Amazon S3, vous pouvez filtrer les données par compte. De même, si vous surveillez les coûts d'utilisation estimés, vous pouvez accéder à la ventilation des coûts estimés pour les comptes de membres individuels.

Outre les tâches communes aux comptes d'administrateur et de membre, vous pouvez effectuer diverses tâches administratives pour votre organisation.

Tâches

- Ajouter des comptes de membres Amazon Macie à une organisation
- Suspension d'Amazon Macie pour les comptes des membres d'une organisation
- Supprimer les comptes membres d'Amazon Macie d'une organisation

En tant qu'administrateur Macie d'une organisation, vous pouvez effectuer ces tâches à l'aide de la console Amazon Macie ou de l'API Amazon Macie. Si vous préférez utiliser la console, vous devez être autorisé à effectuer l' AWS Organizations action suivante : `organizations:ListAccounts` Cette action vous permet de récupérer et d'afficher des informations sur les comptes qui font partie de votre organisation dans AWS Organizations.

Ajouter des comptes de membres Amazon Macie à une organisation

Dans certains cas, vous devrez peut-être ajouter manuellement un compte en tant que compte de membre Macie. C'est le cas des comptes que vous avez précédemment supprimés (dissociés) en tant que comptes membres. C'est également le cas si vous n'avez pas configuré Macie pour activer et ajouter automatiquement de nouveaux comptes de membres lorsque des comptes sont ajoutés à votre organisation dans AWS Organizations.

Lorsque vous ajoutez un compte en tant que compte membre Macie :

- Macie est actuellement activé pour le compte Région AWS, s'il n'est pas déjà activé dans la région.
- Le compte est associé à votre compte administrateur Macie en tant que compte membre dans la région. Le compte membre ne reçoit aucune invitation ou autre notification indiquant que vous avez établi cette relation entre vos comptes.
- La découverte automatique des données sensibles peut être activée pour le compte dans la région. Cela dépend des paramètres de configuration que vous avez spécifiés pour l'organisation. Pour plus d'informations, consultez Configuration de la découverte automatique des données sensibles.

Notez que vous ne pouvez pas ajouter un compte déjà associé à un autre compte administrateur Macie. Le compte doit d'abord se dissocier de son compte administrateur actuel. De plus, vous ne pouvez pas ajouter le compte AWS Organizations de gestion en tant que compte membre à moins que Macie ne soit déjà activé pour le compte. Pour en savoir plus sur les exigences supplémentaires, voirConsidérations et recommandations relatives à l'utilisation d'Amazon Macie avec AWS Organizations.

Pour ajouter un compte de membre Macie à une organisation

Pour ajouter un ou plusieurs comptes de membre Macie à votre organisation, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie.

Console

Suivez ces étapes pour ajouter un ou plusieurs comptes de membre Macie à l'aide de la console Amazon Macie.

Pour ajouter un compte de membre Macie

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.

2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez ajouter un compte membre.
3. Dans le panneau de navigation, choisissez Accounts (Comptes). La page Comptes s'ouvre et affiche un tableau des comptes associés à votre compte.
4. (Facultatif) Pour identifier plus facilement les comptes qui font partie de votre organisation AWS Organizations et qui ne sont pas des comptes membres de Macie, utilisez le champ de filtre situé au-dessus du tableau des comptes pour ajouter les conditions de filtre suivantes :

   - Type = Organisation
   - Statut = Non membre

   Pour afficher également les comptes que vous avez précédemment supprimés et que vous souhaiteriez peut-être ajouter en tant que comptes membres, ajoutez également une condition de filtre Status = Removed.
5. Dans le tableau Comptes, cochez la case correspondant à chaque compte que vous souhaitez ajouter en tant que compte membre.
6. Dans le menu Actions, choisissez Ajouter un membre.
7. Confirmez que vous souhaitez ajouter les comptes sélectionnés en tant que comptes membres.

Une fois que vous avez confirmé vos sélections, le statut des comptes sélectionnés passe à Activation en cours, puis à Activé dans l'inventaire de votre compte.

Répétez les étapes précédentes dans chaque région supplémentaire dans laquelle vous souhaitez ajouter un compte membre.

API

Pour ajouter un ou plusieurs comptes de membre Macie par programmation, utilisez le CreateMemberfonctionnement de l'API Amazon Macie.

Lorsque vous soumettez votre demande, utilisez les paramètres pris en charge pour spécifier l'identifiant de compte à 12 chiffres et l'adresse e-mail de chaque compte Compte AWS que vous souhaitez ajouter. Spécifiez également la région à laquelle s'applique la demande. Pour ajouter un compte dans d'autres régions, soumettez votre demande dans chaque région supplémentaire.

Pour récupérer l'ID de compte et l'adresse e-mail d'un compte à ajouter, vous pouvez corréler le résultat du ListAccountsfonctionnement de l' AWS Organizations API et le

ListMembersfonctionnement de l'API Amazon Macie. Pour le ListMembers fonctionnement de l'API Macie, incluez le `onlyAssociated` paramètre dans votre demande et définissez la valeur du paramètre sur`false`. Si l'opération aboutit, Macie renvoie un `members` tableau qui fournit des détails sur tous les comptes associés à votre compte administrateur Macie dans la région spécifiée, y compris les comptes qui ne sont pas actuellement des comptes membres. Notez ce qui suit dans le tableau :

- Si la valeur de la `relationshipStatus` propriété d'un compte ne l'est pas`Enabled`, le compte est associé à votre compte mais il ne s'agit pas d'un compte de membre Macie.
- Si un compte n'est pas inclus dans le tableau mais est inclus dans le résultat du ListAccounts fonctionnement de l' AWS Organizations API, le compte fait partie de votre organisation AWS Organizations mais n'est pas associé à votre compte et n'est donc pas un compte membre de Macie.

Pour ajouter un compte membre à l'aide de AWS CLI, exécutez la commande create-member. Utilisez le `region` paramètre pour spécifier la région dans laquelle vous souhaitez ajouter le compte. Utilisez les `account` paramètres pour spécifier l'ID de compte et l'adresse e-mail de chaque compte à ajouter. Par exemple :

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"123456789012\",\"email\":\"janedoe@example.com\"}
```

Où us-east-1 est la région dans laquelle ajouter le compte en tant que compte membre (la région USA Est (Virginie du Nord)), et les paramètres spécifient l'ID account du compte (123456789012) et l'adresse e-mail (janedoe@example.com) du compte.

Si votre demande aboutit, le statut (`relationshipStatus`) du compte spécifié est reporté `Enabled` à l'inventaire de votre compte.

Suspension d'Amazon Macie pour les comptes des membres d'une organisation

En tant qu'administrateur Macie d'une organisation dans AWS Organizations, vous pouvez suspendre Macie pour un compte de membre de votre organisation. Dans ce cas, vous pouvez également réactiver Macie pour le compte ultérieurement.

Lorsque vous suspendez Macie pour un compte de membre :

- Macie perd actuellement Région AWS l'accès aux données Amazon S3 du compte et cesse de les fournir.
- Macie cesse d'effectuer toutes les activités liées au compte dans la Région. Cela inclut la surveillance des compartiments S3 à des fins de sécurité et de contrôle d'accès, la découverte automatique des données sensibles et l'exécution des tâches de découverte de données sensibles en cours.
- Macie annule toutes les tâches de découverte de données sensibles créées par le compte dans la région. Une tâche ne peut pas être reprise ou redémarrée après son annulation. Si vous avez créé des tâches pour analyser les données détenues par le compte du membre, Macie n'annule pas vos tâches. Au lieu de cela, les tâches ignorent les ressources détenues par le compte.

Lorsqu'un compte est suspendu, Macie conserve l'identifiant de session Macie, les paramètres et les ressources du compte dans la région applicable. Par exemple, les résultats du compte restent intacts et ne sont pas affectés pendant 90 jours au maximum. Votre organisation n'a pas à payer de frais Macie pour le compte dans la région applicable tant que Macie est suspendu pour le compte dans cette région.

Pour suspendre Macie pour un compte de membre dans une organisation

Pour suspendre Macie pour un compte membre d'une organisation, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie.

Console

Suivez ces étapes pour suspendre Macie pour un compte de membre à l'aide de la console Amazon Macie.

Pour suspendre Macie pour un compte de membre

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez suspendre Macie pour le compte du membre.
3. Dans le panneau de navigation, choisissez Accounts (Comptes). La page Comptes s'ouvre et affiche un tableau des comptes associés à votre compte.
4. Dans le tableau Comptes, cochez la case correspondant au compte que vous souhaitez suspendre.
5. Dans le menu Actions, choisissez Suspendre Macie.

6. Confirmez que vous souhaitez suspendre Macie pour le compte.

Une fois que vous avez confirmé la suspension, le statut du compte passe à Suspendu (suspendu) dans l'inventaire de votre compte.

Répétez les étapes précédentes dans chaque région supplémentaire dans laquelle vous souhaitez suspendre Macie pour le compte.

API

Pour suspendre Macie pour un compte membre par programmation, utilisez le UpdateMemberSessionfonctionnement de l'API Amazon Macie.

Lorsque vous soumettez votre demande, utilisez le `id` paramètre pour spécifier l'identifiant de compte à 12 chiffres pour Compte AWS lequel vous souhaitez suspendre Macie. Pour le `status` paramètre, spécifiez `PAUSED` le nouveau statut du compte Macie. Spécifiez également la région à laquelle s'applique la demande. Pour suspendre le compte dans d'autres régions, soumettez votre demande dans chaque région supplémentaire.

Pour récupérer l'identifiant du compte à suspendre, vous pouvez utiliser l'ListMembersAPI Amazon Macie. Dans ce cas, pensez à filtrer les résultats en incluant le `onlyAssociated` paramètre dans votre demande. Si vous définissez la valeur de ce paramètre sur`true`, Macie renvoie un `members` tableau qui fournit des détails uniquement sur les comptes actuellement membres.

Pour suspendre Macie pour un compte de membre à l'aide de AWS CLI, exécutez la update-member-sessioncommande. Utilisez le `region` paramètre pour spécifier la région dans laquelle vous souhaitez suspendre Macie et utilisez le `id` paramètre pour spécifier l'ID de compte pour lequel Compte AWS vous souhaitez suspendre Macie. Pour le paramètre `status`, spécifiez `PAUSED`. Par exemple :

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status
 PAUSED
```

Où *`us-east-1`* est la région dans laquelle Macie doit être suspendue (région des États-Unis de l'Est (Virginie du Nord)), 123456789012 est l'identifiant du compte pour lequel Macie doit être suspendu et le nouveau statut de Macie pour le compte. `PAUSED`

Si votre demande aboutit, Macie renvoie une réponse vide et le statut du compte spécifié est reporté `Paused` dans l'inventaire de votre compte.

Supprimer les comptes membres d'Amazon Macie d'une organisation

Si vous ne souhaitez plus accéder aux paramètres, aux données et aux ressources de Macie pour un compte de membre, vous pouvez supprimer le compte en tant que compte de membre Macie. Pour ce faire, dissociez le compte de votre compte administrateur Macie. Notez que vous êtes le seul à pouvoir le faire pour un compte membre. Un compte AWS Organizations membre ne peut pas être dissocié de son compte administrateur Macie.

Lorsque vous supprimez un compte de membre Macie, Macie reste activé pour le compte en cours. Région AWS Cependant, le compte est dissocié de votre compte administrateur Macie et devient un compte Macie autonome. Cela signifie que vous perdez l'accès à tous les paramètres, données et ressources Macie du compte, y compris les métadonnées et les conclusions des politiques relatives aux données Amazon S3 du compte. Cela signifie également que vous ne pouvez plus utiliser Macie pour découvrir des données sensibles dans les compartiments S3 détenus par le compte. Si vous avez déjà créé des tâches de découverte sensibles à cette fin, les tâches ignorent les compartiments détenus par le compte. Si vous avez activé la découverte automatique des données sensibles pour le compte, vous et le compte du membre perdez l'accès aux données statistiques, aux données d'inventaire et aux autres informations produites et fournies directement par Macie lors de la découverte automatique du compte.

Une fois que vous avez supprimé un compte de membre Macie, celui-ci continue d'apparaître dans l'inventaire de votre compte. Macie n'informe pas le propriétaire du compte que vous avez supprimé le compte. Vous pourrez ajouter le compte à nouveau à votre organisation ultérieurement. Si vous ajoutez le compte et activez la découverte automatique des données sensibles dans un délai de 30 jours, vous retrouvez également l'accès aux données et informations que Macie avait précédemment produites et fournies directement lors de la découverte automatique du compte.

Pour supprimer un compte de membre Macie d'une organisation

Pour supprimer un compte de membre Macie de votre organisation, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie.

Console

Suivez ces étapes pour supprimer un compte de membre Macie à l'aide de la console Amazon Macie.

Pour supprimer un compte de membre Macie

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.

2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez supprimer le compte de membre.
3. Dans le panneau de navigation, choisissez Accounts (Comptes). La page Comptes s'ouvre et affiche un tableau des comptes associés à votre compte.
4. Dans le tableau Comptes, cochez la case correspondant au compte que vous souhaitez supprimer en tant que compte membre.
5. Dans le menu Actions, choisissez Dissocier le compte.
6. Confirmez que vous souhaitez supprimer le compte sélectionné en tant que compte membre.

Une fois que vous avez confirmé votre sélection, le statut du compte passe à Supprimé (dissocié) dans l'inventaire de votre compte.

Répétez les étapes précédentes dans chaque région supplémentaire dans laquelle vous souhaitez supprimer le compte de membre.

API

Pour supprimer un compte de membre Macie par programmation, utilisez l'API DisassociateMemberAmazon Macie.

Lorsque vous soumettez votre demande, utilisez le `id` paramètre pour spécifier l' Compte AWS identifiant à 12 chiffres du compte membre à supprimer. Spécifiez également la région à laquelle s'applique la demande. Pour supprimer le compte dans d'autres régions, soumettez votre demande dans chaque région supplémentaire.

Pour récupérer l'identifiant du compte membre à supprimer, vous pouvez utiliser ListMembersl'API Amazon Macie. Dans ce cas, pensez à filtrer les résultats en incluant le `onlyAssociated` paramètre dans votre demande. Si vous définissez la valeur de ce paramètre sur`true`, Macie renvoie un `members` tableau qui fournit des détails uniquement sur les comptes actuellement membres de Macie.

Pour supprimer un compte membre Macie à l'aide de AWS CLI, exécutez la commande disassociate-member. Utilisez le `region` paramètre pour spécifier la région dans laquelle vous souhaitez supprimer le compte. Utilisez le `id` paramètre pour spécifier l'ID de compte du membre à supprimer. Par exemple :

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

Où *us-east-1* est la région dans laquelle le compte doit être supprimé (région USA Est (Virginie du Nord)) *et* 123456789012 est l'identifiant du compte à supprimer.

Si votre demande aboutit, Macie renvoie une réponse vide et le statut du compte spécifié est reporté `Removed` dans l'inventaire de votre compte.

Désignation d'un compte administrateur Amazon Macie différent pour une organisation

Une fois qu'une AWS Organizations organisation est intégrée et configurée dans Amazon Macie, le compte de AWS Organizations gestion peut désigner un autre compte en tant que compte administrateur Macie délégué pour l'organisation.

En tant qu'utilisateur du compte de AWS Organizations gestion d'une organisation, vérifiez que vous répondez aux exigences d'autorisation suivantes avant de désigner un autre compte administrateur Macie pour votre organisation :

- Vous devez disposer des mêmes autorisations que celles requises pour désigner initialement un compte administrateur Macie pour votre organisation. Vous devez également être autorisé à effectuer l' AWS Organizations action suivante : `organizations:DeregisterDelegatedAdministrator` Cette action supplémentaire vous permet de supprimer la désignation actuelle.
- Si votre compte est actuellement un compte de membre Macie, l'administrateur Macie actuel doit supprimer votre compte en tant que compte de membre Macie. Sinon, vous ne serez pas autorisé à accéder aux opérations de Macie pour désigner un autre compte administrateur. Une fois que vous avez désigné un nouveau compte administrateur, le nouvel administrateur Macie peut à nouveau ajouter votre compte en tant que compte membre Macie.

Si votre organisation utilise Macie à plusieurs reprises Régions AWS, assurez-vous également de modifier le compte d'administrateur Macie délégué dans chaque région dans laquelle votre organisation utilise Macie. Le compte administrateur Macie délégué doit être le même dans toutes ces régions. Si vous gérez plusieurs organisations dans AWS Organizations, notez également qu'un compte ne peut être le compte d'administrateur Macie délégué que pour une seule organisation à la fois. Pour en savoir plus sur les exigences supplémentaires, voirConsidérations et recommandations relatives à l'utilisation d'Amazon Macie avec AWS Organizations.

> **Note**
>
> Lorsque vous désignez un autre compte administrateur Macie pour votre organisation, vous désactivez également l'accès aux données statistiques existantes, aux données d'inventaire et aux autres informations produites et fournies directement par Macie lors de la découverte automatique des données sensibles pour les comptes de l'organisation. Le nouveau compte administrateur Macie ne peut pas accéder aux données existantes. Si vous modifiez la désignation et que le nouvel administrateur Macie active la découverte automatique des comptes, Macie génère et gère de nouvelles données lorsqu'il effectue la découverte automatique des comptes.

Pour désigner un compte administrateur Macie différent pour votre organisation

Pour désigner un compte administrateur Macie différent pour votre organisation, vous pouvez utiliser la console Amazon Macie ou une combinaison d'Amazon Macie et d'API. AWS Organizations Seul un utilisateur du compte de AWS Organizations gestion peut modifier la désignation de son organisation.

Console

Pour modifier la désignation à l'aide de la console Amazon Macie, procédez comme suit.

Pour désigner un autre compte administrateur Macie

1. Connectez-vous à l' AWS Management Console aide de votre compte AWS Organizations de gestion.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez modifier la désignation.
3. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
4. Procédez de l'une des manières suivantes, selon que Macie est activé ou non pour votre compte de gestion dans la région actuelle :
   - Si Macie n'est pas activé, choisissez Commencer sur la page d'accueil.
   - Si Macie est activé, choisissez Paramètres dans le volet de navigation.
5. Sous Administrateur délégué, choisissez Supprimer. Pour modifier la désignation, vous devez d'abord supprimer la désignation actuelle.
6. Confirmez que vous souhaitez supprimer la désignation actuelle.

7. Sous Administrateur délégué, entrez l'identifiant de compte à 12 chiffres Compte AWS pour le désigner comme nouveau compte administrateur Macie pour l'organisation.
8. Choisisssez Delegate (Déléguer).

Répétez les étapes précédentes dans chaque région supplémentaire dans laquelle vous avez intégré Macie. AWS Organizations

API

Pour modifier la désignation par programmation, vous devez utiliser deux opérations de l'API Amazon Macie et une opération de l'API. AWS Organizations En effet, vous devez supprimer la désignation actuelle à la fois dans Macie et AWS Organizations avant de soumettre la nouvelle désignation.

Pour supprimer la désignation actuelle, procédez comme suit :

1. Utilisez le DisableOrganizationAdminAccountfonctionnement de l'API Macie. Pour le `adminAccountId` paramètre requis, spécifiez l'identifiant de compte à 12 chiffres pour Compte AWS le compte actuellement désigné comme le compte administrateur Macie de l'organisation.
2. Utilisez le DeregisterDelegatedAdministratorfonctionnement de l' AWS Organizations API. Pour le `AccountId` paramètre, spécifiez l'ID de compte à 12 chiffres du compte actuellement désigné comme compte administrateur Macie pour l'organisation. Cette valeur doit correspondre à l'identifiant de compte que vous avez spécifié dans la demande Macie précédente. Pour le `ServicePrincipal` paramètre, spécifiez le principal de service Macie (`macie.amazonaws.com`).

Après avoir supprimé la désignation actuelle, soumettez la nouvelle désignation en utilisant le EnableOrganizationAdminAccountfonctionnement de l'API Macie. Pour le `adminAccountId` paramètre requis, spécifiez l'identifiant de compte à 12 chiffres Compte AWS à désigner comme nouveau compte administrateur Macie pour l'organisation.

Pour modifier la désignation à l'aide du AWS CLI, exécutez la disable-organization-admin-accountcommande de l'API Macie et la deregister-delegated-administratorcommande de l' AWS Organizations API. Ces commandes suppriment la désignation actuelle dans Macie et AWS Organizations, respectivement. Pour les `account-id` paramètres `admin-account-id` et, spécifiez l'identifiant de compte à 12 chiffres Compte AWS à supprimer en tant que compte

administrateur Macie actuel. Utilisez le `region` paramètre pour spécifier la région à laquelle s'applique la suppression. Par exemple :

```
C:\> aws macie2 disable-organization-admin-account --region us-east-1 --admin-
account-id 111122223333 && aws organizations deregister-delegated-administrator --
region us-east-1 --account-id 111122223333 --service-principal macie.amazonaws.com
```

Où :

- *us-east-1* est la région à laquelle s'applique la suppression, la région de l'est des États-Unis (Virginie du Nord).
- *111122223333* est l'identifiant du compte à supprimer en tant que compte administrateur Macie.
- `macie.amazonaws.com`est le directeur du service Macie.

Après avoir supprimé la désignation actuelle, soumettez la nouvelle désignation en exécutant la enable-organization-admin-accountcommande de l'API Macie. Pour le `admin-account-id` paramètre, spécifiez l'identifiant de compte à 12 chiffres Compte AWS à désigner comme nouveau compte administrateur Macie pour l'organisation. Utilisez le `region` paramètre pour spécifier la région à laquelle la désignation s'applique. Par exemple :

```
C:\> aws macie2 enable-organization-admin-account --region us-east-1 --admin-
account-id 444455556666
```

Où *us-east-1* est la région à laquelle s'applique la désignation (la région USA Est (Virginie du Nord)) *et* 444455556666 est l'identifiant du compte à désigner comme nouveau compte administrateur Macie.

Désactivation de l'intégration d'Amazon Macie avec AWS Organizations

Une fois qu'une AWS Organizations organisation est intégrée à Amazon Macie, le compte AWS Organizations de gestion peut ensuite désactiver l'intégration. En tant qu'utilisateur du compte de AWS Organizations gestion, vous pouvez le faire en désactivant l'accès aux services sécurisés pour Macie in. AWS Organizations

Lorsque vous désactivez l'accès aux services sécurisés pour Macie, les événements suivants se produisent :

- Macie perd son statut de service de confiance en AWS Organizations.
- Le compte administrateur Macie de l'organisation perd l'accès à tous les paramètres, données et ressources Macie pour tous les comptes de membres Macie. Régions AWS
- Tous les comptes des membres Macie deviennent des comptes Macie autonomes. Si Macie a été activé pour un compte membre dans une ou plusieurs régions, Macie continue d'être activé pour le compte dans ces régions. Toutefois, le compte n'est plus associé à un compte administrateur Macie dans aucune région. En outre, le compte perd l'accès aux données statistiques, aux données d'inventaire et aux autres informations produites et fournies directement par Macie lors de la découverte automatique de données sensibles pour le compte.

Pour plus d'informations sur les conséquences de la désactivation de l'accès aux services sécurisés, consultez la section Utilisation AWS Organizations avec d'autres personnes Services AWS dans le Guide de l'AWS Organizations utilisateur.

Pour désactiver l'accès sécurisé aux services pour Macie

Pour désactiver l'accès aux services sécurisés, vous pouvez utiliser la AWS Organizations console ou l' AWS Organizations API. Seul un utilisateur du compte de AWS Organizations gestion peut désactiver l'accès aux services sécurisés pour Macie. Pour plus de détails sur les autorisations dont vous avez besoin, consultez la section Autorisations requises pour désactiver l'accès sécurisé dans le Guide de AWS Organizations l'utilisateur.

Avant de désactiver l'accès aux services sécurisés, contactez éventuellement l'administrateur Macie délégué de votre organisation afin de suspendre ou de désactiver Macie pour les comptes des membres et de nettoyer les ressources Macie pour ces comptes.

Console

Pour désactiver l'accès aux services sécurisés à l'aide de la AWS Organizations console, procédez comme suit.

Pour désactiver l'accès au service approuvé

1. Connectez-vous à l' AWS Management Console aide de votre compte AWS Organizations de gestion.
2. Ouvrez la AWS Organizations console à l'adresse https://console.aws.amazon.com/organizations/.
3. Dans le panneau de navigation, choisissez Services.

4. Dans Services intégrés, sélectionnez Amazon Macie.
5. Choisissez Disable trusted access (Désactiver l'accès approuvé).
6. Confirmez que vous souhaitez désactiver l'accès sécurisé.

API

Pour désactiver l'accès aux services sécurisés par programmation, utilisez l'AWSServiceAccessopération Désactiver de l' AWS Organizations API. Pour le `ServicePrincipal` paramètre, spécifiez le principal de service Macie (`macie.amazonaws.com`).

Pour désactiver l'accès aux services sécurisés à l'aide de AWS Command Line Interface (AWS CLI), exécutez la disable-aws-service-accesscommande de l' AWS Organizations API. Pour le `service-principal` paramètre, spécifiez le principal de service Macie (`macie.amazonaws.com`). Par exemple :

```
C:\> aws organizations disable-aws-service-access --service-principal
 macie.amazonaws.com
```

Gestion des comptes Amazon Macie sur invitation

Vous pouvez gérer de manière centralisée plusieurs comptes Amazon Macie de deux manières : en intégrant Macie à des invitations d'adhésion AWS Organizations ou en utilisant des invitations d'adhésion. Si vous utilisez des invitations d'adhésion, un administrateur Macie désigné peut gérer Macie pour un maximum de 1 000 comptes. L'administrateur peut également accéder aux données des comptes. Pour plus de détails sur les tâches que les administrateurs peuvent effectuer, consultezComprendre la relation entre les comptes d'administrateur et de membre d'Amazon Macie.

Dans une organisation basée sur des invitations, vous associez des comptes Macie entre eux en envoyant et en acceptant des invitations d'adhésion dans Macie. Si vous envoyez une invitation et qu'elle est acceptée par un autre compte, vous devenez l'administrateur Macie de l'autre compte et celui-ci devient un compte membre de votre organisation. Si vous recevez et acceptez une invitation, votre compte devient un compte membre et l'administrateur de Macie peut accéder à certains paramètres, données et ressources de Macie pour votre compte.

> **Tip**
>
> Si vous créez une organisation basée sur des invitations dans Macie, vous pouvez ensuite passer à l'utilisation à la place. AWS Organizations Vous pouvez également utiliser les deux méthodes simultanément pour gérer plusieurs comptes Macie. Par exemple, si votre AWS environnement inclut des comptes de test, vous pouvez exclure les comptes de votre organisation AWS Organizations et les gérer séparément sur invitation.

Les rubriques de cette section expliquent comment créer une organisation basée sur des invitations et y participer, ainsi que comment effectuer diverses tâches administratives pour l'organisation.

Rubriques

- Considérations et recommandations pour les organisations basées sur des invitations dans Amazon Macie
- Création et gestion d'une organisation basée sur des invitations dans Amazon Macie
- Révision des comptes Amazon Macie pour une organisation basée sur des invitations
- Désignation d'un compte administrateur Amazon Macie différent pour une organisation basée sur des invitations
- Gérer votre adhésion à une organisation basée sur des invitations dans Amazon Macie

Considérations et recommandations pour les organisations basées sur des invitations dans Amazon Macie

Avant de créer ou de commencer à gérer une organisation basée sur des invitations dans Amazon Macie, tenez compte des exigences et recommandations suivantes. Assurez-vous également de bien comprendre la relation entre les comptes administrateur et membre de Macie.

Rubriques

- Choisir un compte administrateur Macie
- Envoyer des invitations et gérer les comptes des membres Macie
- Répondre aux invitations aux membres et les gérer
- Transition vers AWS Organizations

Choisir un compte administrateur Macie

Lorsque vous déterminez quel compte doit être le compte administrateur Macie de l'organisation, gardez les points suivants à l'esprit :

- Une organisation ne peut avoir qu'un seul compte administrateur Macie.
- Un compte ne peut pas être un compte administrateur Macie et un compte membre à la fois.
- Macie est un service régional. Cela signifie que l'association entre un compte administrateur Macie et un compte membre est régionale : l'association n'existe Région AWS que dans le cas où une invitation est envoyée et acceptée. Par exemple, si l'administrateur Macie envoie des invitations dans la région USA Est (Virginie du Nord) et que ces invitations sont acceptées, l'administrateur Macie peut gérer les comptes des membres uniquement dans cette région.
- Pour gérer de manière centralisée plusieurs comptes Macie Régions AWS, l'administrateur Macie doit se connecter à chaque région dans laquelle l'organisation utilise actuellement ou prévoit d'utiliser Macie, et envoyer des invitations aux comptes appropriés dans chacune de ces régions. Pour obtenir la liste des régions dans lesquelles Macie est actuellement disponible, consultez la section Points de terminaison et quotas Amazon Macie dans le. Références générales AWS
- Un compte membre ne peut être associé qu'à un seul compte administrateur Macie à la fois. Si votre organisation utilise Macie dans plusieurs régions, cela signifie que le compte administrateur Macie doit être le même dans toutes ces régions. Toutefois, les comptes administrateur et membre doivent envoyer et accepter les invitations séparément dans chaque région.

Si l'administrateur Macie Compte AWS est suspendu, isolé ou fermé, tous les comptes de membre associés sont automatiquement supprimés en tant que comptes de membre, mais Macie continue d'être activé pour ces comptes. Les comptes deviennent des comptes Macie autonomes. Si la découverte automatique des données sensibles a été activée pour le compte d'un membre, elle est désactivée pour le compte. Cela désactive également l'accès aux données statistiques, aux données d'inventaire et aux autres informations produites et fournies directement par Macie lors de la découverte automatique du compte. Au bout de 30 jours, ces données expirent et Macie les supprime définitivement. Pour rétablir l'accès aux données avant leur expiration, restaurez celui de l'administrateur Macie Compte AWS, puis utilisez ce compte pour créer et configurer à nouveau l'organisation.

Envoyer des invitations et gérer les comptes des membres Macie

En tant qu'administrateur Macie d'une organisation basée sur des invitations, gardez à l'esprit les points suivants lorsque vous envoyez des invitations et gérez des comptes au sein de l'organisation :

- Si vous envoyez une invitation, les données associées peuvent être transférées Régions AWS. C'est le cas car Macie vérifie l'adresse e-mail du compte destinataire à l'aide d'un service de vérification des e-mails qui fonctionne uniquement dans la région de l'est des États-Unis (Virginie du Nord).
- Vous pouvez envoyer une invitation à n'importe quel compte actif Compte AWS, y compris aux comptes qui n'ont pas activé Macie. Toutefois, pour accepter ou refuser une invitation, le compte destinataire doit activer Macie dans la région d'où l'invitation a été envoyée.
- Un compte administrateur Macie ne peut pas être associé à plus de 1 000 comptes par compte. Région AWS Cela inclut les comptes qui n'ont pas encore répondu aux invitations. Si votre compte atteint ce quota, vous ne pouvez pas ajouter ou inviter de comptes supplémentaires tant que vous n'avez pas supprimé le nombre nécessaire de comptes associés, reçu le nombre nécessaire d'invitations refusées ou une combinaison des deux.

  Pour déterminer le nombre de comptes actuellement associés à votre compte, vous pouvez utiliser la page Comptes de la console Amazon Macie ou le ListMembersfonctionnement de l'API Amazon Macie. Pour plus d'informations, consultez Révision des comptes Amazon Macie pour une organisation basée sur des invitations.
- Un compte ne peut être associé qu'à un seul compte administrateur Macie à la fois. Cela signifie qu'un compte ne peut pas accepter votre invitation s'il est déjà associé à un autre compte administrateur Macie. Le compte doit d'abord se dissocier de son compte administrateur Macie actuel.
- Dans une organisation basée sur des invitations, un compte membre peut se dissocier de son compte administrateur Macie à tout moment. Dans ce cas, Macie continue d'être activé pour le compte, mais celui-ci devient un compte Macie autonome. Macie ne vous avertit pas si un compte membre se dissocie de votre compte administrateur. Cependant, le compte continue d'apparaître dans l'inventaire de votre compte et il a le statut de membre démissionnaire.
- Si vous supprimez un compte membre de votre organisation, Macie continue d'être activé pour ce compte. Le compte devient un compte Macie autonome.

Répondre aux invitations aux membres et les gérer

En tant que destinataire d'une invitation ou membre d'une organisation basée sur des invitations, gardez à l'esprit les points suivants lorsque vous répondez aux invitations que vous recevez et que vous les gérez :

- Avant d'accepter une invitation, assurez-vous de bien comprendre la relation entre les comptes administrateur et membre de Macie.
- Votre compte ne peut être associé qu'à un seul compte administrateur Macie à la fois. Si vous acceptez une invitation et souhaitez ensuite rejoindre une autre organisation (par invitation ou via AWS Organizations), vous devez d'abord dissocier votre compte de son compte administrateur Macie actuel. Vous pouvez ensuite rejoindre l'autre organisation.
- Pour accepter ou refuser une invitation, vous devez activer Macie dans le pays d' Région AWS où l'invitation a été envoyée. Le compte qui a envoyé l'invitation ne peut pas activer Macie dans cette région pour vous. Le refus d'une invitation est facultatif. Si vous refusez une invitation, vous pouvez éventuellement désactiver Macie dans la région applicable après avoir décliné l'invitation.
- Si vous êtes administrateur Macie, vous ne pouvez pas accepter une invitation à devenir un compte membre. Un compte ne peut pas être à la fois administrateur et compte membre Macie. Pour devenir un compte membre, vous devez d'abord dissocier votre compte de tous ses comptes membres en supprimant tous les comptes membres de votre organisation actuelle.
- Macie est un service régional. Si vous acceptez une invitation, l'association entre votre compte et le compte administrateur Macie est régionale : l'association n'existe Région AWS que dans le pays d'où l'invitation a été envoyée et acceptée.
- Si vous utilisez Macie dans plusieurs régions, le compte administrateur Macie de votre compte doit être le même dans toutes ces régions. Cependant, l'administrateur Macie doit vous envoyer des invitations séparément dans chaque région, et vous devez accepter les invitations séparément dans chaque région.
- Vous pouvez dissocier votre compte d'un compte administrateur Macie à tout moment. De même, votre administrateur Macie peut supprimer votre compte de son organisation à tout moment. Si l'un ou l'autre se produit :
  - Macie est toujours activé pour votre compte. Votre compte devient un compte Macie autonome.
  - La découverte automatique des données sensibles est désactivée pour votre compte, si elle a été activée. Cela désactive également l'accès aux données statistiques existantes, aux données d'inventaire et aux autres informations produites et fournies directement par Macie lors de la découverte automatique de votre compte. Vous pouvez réactiver la découverte automatique pour votre compte. Toutefois, cela ne rétablit pas l'accès aux données existantes. Au lieu de cela, Macie génère et gère de nouvelles données tout en effectuant la découverte automatique de votre compte.

Transition vers AWS Organizations

Après avoir créé une organisation basée sur des invitations dans Macie, vous pouvez passer à l'utilisation à la place. AWS Organizations Pour simplifier la transition, nous vous recommandons de désigner le compte administrateur existant basé sur des invitations comme compte administrateur Macie de l'organisation dans. AWS Organizations

Dans ce cas, tous les comptes de membres actuellement associés restent membres. Si un compte membre fait partie de l'organisation dans AWS Organizations, l'association du compte passe automatiquement de By invitation à Via AWS Organizations in Macie. Si le compte d'un membre ne fait pas partie de l'organisation dans AWS Organizations, l'association du compte continue d'être sur invitation. Dans les deux cas, les comptes continuent d'être associés au compte administrateur Macie en tant que comptes de membre.

Nous recommandons cette approche car un compte membre ne peut être associé qu'à un seul compte administrateur Macie à la fois. Si vous désignez un autre compte comme compte administrateur Macie pour une organisation dans AWS Organizations, l'administrateur désigné ne pourra pas gérer les comptes déjà associés à un autre compte administrateur Macie sur invitation. Chaque compte membre doit d'abord se dissocier de son compte administrateur actuel, basé sur des invitations. Ce n'est qu'alors que l'administrateur Macie de l' AWS Organizations organisation pourra ajouter le compte du membre à son organisation et commencer à gérer Macie pour le compte.

Après avoir intégré Macie à Macie AWS Organizations et configuré votre organisation dans Macie, vous pouvez éventuellement désigner un compte administrateur Macie différent pour l'organisation. Vous pouvez également continuer à utiliser des invitations pour associer et gérer des comptes de membres qui ne font pas partie de votre organisation AWS Organizations.

Pour plus d'informations sur l'intégration de Macie à AWS Organizations, consultezGestion des comptes Amazon Macie avec AWS Organizations.

Création et gestion d'une organisation basée sur des invitations dans Amazon Macie

Pour créer une organisation basée sur des invitations dans Amazon Macie, vous devez d'abord déterminer le compte que vous souhaitez utiliser comme compte administrateur Macie pour l'organisation. Vous utilisez ensuite ce compte pour ajouter des comptes de membre : vous envoyez des invitations d'adhésion à d'autres personnes Comptes AWS, en les invitant à rejoindre l'organisation en tant que comptes membres Macie actuels. Région AWS Pour créer l'organisation

dans plusieurs régions, envoyez des invitations d'adhésion depuis chaque région dans laquelle les autres comptes utilisent actuellement ou prévoient d'utiliser Macie.

Lorsqu'un compte accepte une invitation, il devient un compte membre Macie associé au compte administrateur Macie dans la région applicable. Le compte administrateur Macie peut ensuite accéder à certains paramètres, données et ressources Macie pour le compte membre dans cette région.

En tant qu'administrateur Macie d'une organisation basée sur des invitations, vous pouvez consulter les données d'inventaire d'Amazon Simple Storage Service (Amazon S3) et les conclusions relatives aux politiques relatives aux comptes membres. Vous pouvez également activer la découverte automatique des données sensibles et exécuter des tâches de découverte de données sensibles pour détecter les données sensibles dans les compartiments S3 détenus par les comptes membres. Pour une liste détaillée des tâches que vous pouvez effectuer, consultezComprendre la relation entre les comptes d'administrateur et de membre d'Amazon Macie.

Par défaut, Macie vous donne une visibilité sur les données et les ressources pertinentes pour l'ensemble de votre organisation. Vous pouvez également passer en revue les données et les ressources des comptes individuels de votre organisation. Par exemple, si vous utilisez le tableau de bord récapitulatif pour évaluer le niveau de sécurité de votre organisation sur Amazon S3, vous pouvez filtrer les données par compte. De même, si vous surveillez les coûts d'utilisation estimés, vous pouvez accéder à la ventilation des coûts estimés pour les comptes de membres individuels.

Outre les tâches communes aux comptes d'administrateur et de membre, vous pouvez effectuer de manière centralisée diverses tâches administratives pour votre organisation. Avant d'effectuer ces tâches, il est conseillé de passer en revue les considérations et les recommandations relatives à la gestion des organisations basées sur des invitations dans Macie.

Tâches

- Ajouter des comptes de membres Amazon Macie à une organisation basée sur une invitation
- Suspension d'Amazon Macie pour les comptes membres d'une organisation basée sur une invitation
- Supprimer les comptes de membres Amazon Macie d'une organisation basée sur une invitation
- Supprimer des associations avec d'autres comptes

Ajouter des comptes de membres Amazon Macie à une organisation basée sur une invitation

En tant qu'administrateur Macie d'une organisation basée sur des invitations, vous ajoutez des comptes de membres à votre organisation en effectuant deux étapes principales :

1. Ajoutez les comptes à l'inventaire de vos comptes dans Macie. Cela permet d'associer les comptes à votre compte.
2. Envoyez des invitations d'adhésion aux comptes.

Lorsqu'un compte accepte votre invitation, il devient un compte membre de votre organisation.

Étape 1 : Ajoutez les comptes

Pour ajouter un ou plusieurs comptes à l'inventaire de votre compte, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie.

Console

Avec la console Amazon Macie, vous pouvez ajouter un compte à la fois ou ajouter plusieurs comptes en même temps en téléchargeant un fichier CSV (valeurs séparées par des virgules). Procédez comme suit pour ajouter un ou plusieurs comptes à l'aide de la console.

Pour ajouter un compte

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez ajouter un compte.
3. Dans le panneau de navigation, choisissez Accounts (Comptes). La page Comptes s'ouvre et affiche un tableau des comptes actuellement associés à votre compte.
4. Choisissez Add accounts.
5. Dans la section Entrez les détails du compte, choisissez Ajouter un compte. Ensuite, procédez comme suit :
   - Pour ID de compte, entrez l'identifiant de compte à 12 chiffres Compte AWS à ajouter.
   - Dans Adresse e-mail, entrez l'adresse e-mail Compte AWS à ajouter.
6. Choisissez Ajouter.

7. Au bas de la page, sélectionnez Next.

Macie ajoute le compte à l'inventaire de votre compte. Le type de compte est Sur invitation et son statut est Créé. Répétez les étapes précédentes dans chaque région supplémentaire dans laquelle vous souhaitez ajouter le compte.

Pour ajouter plusieurs comptes

1. À l'aide d'un éditeur de texte, créez un fichier CSV comme suit :

   a. Ajoutez l'en-tête suivant comme première ligne du fichier : `Account ID,Email`

   b. Pour chaque compte, créez une nouvelle ligne contenant l'identifiant de compte à 12 chiffres Compte AWS à ajouter et l'adresse e-mail du compte. Séparez les entrées par une virgule, par exemple : `111111111111,janedoe@example.com`

      L'adresse e-mail doit correspondre à l'adresse e-mail associée au Compte AWS.

   c. Vérifiez que le contenu du fichier est formaté comme indiqué dans l'exemple suivant, qui contient l'en-tête et les informations requis pour trois comptes :

```
Account ID,Email
111111111111,janedoe@example.com
222222222222,jorgesouza@example.com
333333333333,lijuan@example.com
```

   d. Enregistrez le fichier sur votre ordinateur.

2. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
3. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez ajouter les comptes.
4. Dans le panneau de navigation, choisissez Accounts (Comptes). La page Comptes s'ouvre et affiche un tableau des comptes actuellement associés à votre compte.
5. Choisissez Add accounts.
6. Dans la section Entrez les détails du compte, choisissez Charger la liste (CSV).
7. Choisissez Parcourir, puis sélectionnez le fichier CSV que vous avez créé à l'étape 1.
8. Choisissez Add accounts.
9. Au bas de la page, sélectionnez Next.

Macie ajoute les comptes à l'inventaire de vos comptes. Leur type est Par invitation et leur statut est créé. Répétez les étapes 3 à 8 dans chaque région supplémentaire dans laquelle vous souhaitez ajouter les comptes.

API

Pour ajouter un ou plusieurs comptes par programmation, utilisez l'CreateMemberAPI Amazon Macie. Lorsque vous soumettez votre demande, utilisez les paramètres pris en charge pour spécifier l'identifiant de compte à 12 chiffres et l'adresse e-mail de chacun Compte AWS à ajouter. Spécifiez également la région à laquelle s'applique la demande. Pour ajouter des comptes dans des régions supplémentaires, soumettez la demande dans chaque région supplémentaire.

Pour ajouter des comptes à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande create-member. Utilisez le `region` paramètre pour spécifier la région dans laquelle vous souhaitez ajouter les comptes. Utilisez les `account` paramètres pour spécifier l'ID de compte et l'adresse e-mail de chacun Compte AWS à ajouter. Par exemple :

```
C:\> aws macie2 create-member --region us-east-1 --account={\"accountId\":
\"111111111111\",\"email\":\"janedoe@example.com\"}
```

Où us-east-1 est la région dans laquelle ajouter le compte (la région USA Est (Virginie du Nord)) et les paramètres spécifient l'ID account du compte (111111111111) et l'adresse e-mail (janedoe@example.com) du compte à ajouter.

Si votre demande aboutit, Macie ajoute chaque compte à l'inventaire de votre compte avec un statut de `Created` et vous recevez un résultat similaire à ce qui suit :

```
{
    "arn": "arn:aws:macie2:us-east-1:123456789012:member/111111111111"
}
```

Où se `arn` trouve le nom de ressource Amazon (ARN) de la ressource créée pour l'association entre votre compte et le compte que vous avez ajouté ? Dans cet exemple, `123456789012` il s'agit de l'ID de compte du compte qui a créé l'association et `111111111111` de l'ID de compte du compte ajouté.

Étape 2 : envoyer des invitations d'adhésion aux comptes

Après avoir ajouté un compte à l'inventaire de vos comptes, vous pouvez l'inviter à rejoindre votre organisation en tant que compte membre Macie. Pour ce faire, envoyez une invitation d'adhésion au compte. Lorsque vous envoyez une invitation, un badge de compte et une notification apparaissent sur la console Amazon Macie pour le compte du destinataire, si Macie est activé pour le compte. Macie crée également un AWS Health événement pour le compte.

Selon que vous utilisez la console ou l'API Amazon Macie pour envoyer l'invitation, Macie envoie également l'invitation à l'adresse e-mail que vous avez spécifiée pour le compte du destinataire lorsque vous avez ajouté le compte. Le message électronique indique que vous souhaitez devenir l'administrateur Macie de leur compte, et il inclut l'identifiant de votre compte Compte AWS et celui du Compte AWS destinataire. Le message explique également comment accéder à l'invitation. Vous pouvez éventuellement ajouter du texte personnalisé au message.

Pour envoyer une invitation d'adhésion à un ou plusieurs comptes, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie.

Console

Suivez ces étapes pour envoyer une invitation d'adhésion à l'aide de la console Amazon Macie.

Pour envoyer une invitation d'adhésion

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez envoyer l'invitation.
3. Dans le panneau de navigation, choisissez Accounts (Comptes). La page Comptes s'ouvre et affiche un tableau des comptes actuellement associés à votre compte.
4. Dans le tableau Comptes, cochez la case correspondant à chaque compte auquel vous souhaitez envoyer l'invitation.

> **Tip**
>
> Pour identifier plus facilement les comptes que vous avez ajoutés et auxquels vous n'avez pas encore envoyé d'invitations, vous pouvez filtrer le tableau. Pour ce faire, placez votre curseur dans la zone de filtre située au-dessus du tableau, puis choisissez Status. Choisissez ensuite Status = Created.

5. Dans le menu Actions, choisissez Inviter.
6. (Facultatif) Dans la zone Message, entrez le texte personnalisé que vous souhaitez inclure dans le message électronique contenant l'invitation. Le texte peut contenir jusqu'à 80 caractères alphanumériques.
7. Choisissez Inviter.

Pour envoyer l'invitation en plus Régions AWS, répétez les étapes précédentes dans chaque région supplémentaire.

Une fois que vous avez envoyé l'invitation, le statut du compte du destinataire passe à Vérification par e-mail en cours dans l'inventaire de votre compte. Si Macie peut vérifier l'adresse e-mail d'un compte, le statut du compte passe ensuite à Invité. Si Macie ne parvient pas à vérifier l'adresse, le statut du compte passe à la validation par e-mail. Échec. Dans ce cas, contactez le propriétaire du compte pour obtenir la bonne adresse e-mail. Supprimez ensuite l'association entre vos comptes, ajoutez à nouveau le compte et envoyez à nouveau l'invitation.

Lorsqu'un destinataire accepte une invitation, le statut du compte du destinataire passe à Activé dans l'inventaire de votre compte. Si un destinataire refuse une invitation, le compte du destinataire est dissocié de votre compte et supprimé de l'inventaire de votre compte.

API

Pour envoyer une invitation par programmation, utilisez le CreateInvitationsfonctionnement de l'API Amazon Macie. Lorsque vous soumettez votre demande, utilisez les paramètres pris en charge pour spécifier l'identifiant de compte à 12 chiffres pour chacun des Compte AWS utilisateurs auxquels envoyer l'invitation. Un identifiant de compte doit correspondre à l'identifiant de compte d'un compte figurant dans l'inventaire de votre compte. Dans le cas contraire, une erreur se produit. Spécifiez également la région à partir de laquelle envoyer l'invitation. Pour envoyer l'invitation depuis des régions supplémentaires, soumettez la demande dans chaque région supplémentaire.

Dans votre demande, vous pouvez également indiquer si vous souhaitez envoyer l'invitation sous forme de message électronique et si vous souhaitez inclure un texte personnalisé dans ce message. Si vous choisissez d'envoyer un e-mail, Macie envoie l'invitation à l'adresse e-mail que vous avez spécifiée pour un compte lorsque vous l'avez ajouté à l'inventaire de votre compte. Pour envoyer l'invitation sous forme de message électronique, omettez le `disableEmailNotification` paramètre ou définissez la valeur du paramètre sur. `false` (La valeur par défaut est `false`.) Pour ajouter du texte personnalisé au message, utilisez le

`message` paramètre pour spécifier le texte à ajouter. Le texte peut contenir jusqu'à 80 caractères alphanumériques.

Pour envoyer des invitations à l'aide de AWS CLI, exécutez la commande create-invitations. Utilisez le `region` paramètre pour spécifier la région à partir de laquelle envoyer l'invitation. Utilisez le `account-ids` paramètre pour spécifier l'ID de compte de chacun Compte AWS des destinataires auxquels envoyer l'invitation. Par exemple :

```
C:\> aws macie2 create-invitations --region us-east-1 --account-
ids=[\"111111111111\",\"222222222222\",\"333333333333\"]
```

Où *us-east-1* est la région depuis laquelle envoyer l'invitation (région USA Est (Virginie du Nord)) et le paramètre spécifie les identifiants de compte de trois comptes auxquels envoyer `account-ids` l'invitation. Pour envoyer également une invitation sous forme de message électronique, incluez également le `no-disable-email-notification` paramètre et incluez éventuellement le `message` paramètre pour spécifier le texte personnalisé à ajouter au message.

Une fois que vous avez envoyé l'invitation, le statut de chaque compte destinataire passe à`EmailVerificationInProgress`. Si Macie peut vérifier l'adresse e-mail d'un compte, le statut du compte passe ensuite à`Invited`. Si Macie ne parvient pas à vérifier l'adresse, le statut du compte passe à`EmailVerificationFailed`. Dans ce cas, contactez le titulaire du compte pour obtenir la bonne adresse. Supprimez ensuite l'association entre vos comptes, ajoutez à nouveau le compte et envoyez à nouveau l'invitation.

Lorsqu'un destinataire accepte une invitation, le statut du compte du destinataire passe `Enabled` à l'inventaire de votre compte. Si un destinataire refuse une invitation, le compte du destinataire est dissocié de votre compte et supprimé de l'inventaire de votre compte.

Suspension d'Amazon Macie pour les comptes membres d'une organisation basée sur une invitation

En tant qu'administrateur Macie d'une organisation, vous pouvez suspendre Macie de manière spécifique Région AWS pour les comptes de membres individuels de votre organisation. Notez toutefois que vous ne pouvez pas réactiver Macie pour un compte de membre après l'avoir suspendu. Seul un utilisateur du compte peut ensuite réactiver Macie pour le compte.

Lorsque vous suspendez Macie pour un compte de membre :

- Macie perd l'accès aux données Amazon S3 du compte dans la région et cesse de les fournir.

- Macie cesse d'effectuer toutes les activités liées au compte dans la Région. Cela inclut la surveillance des compartiments S3 à des fins de sécurité et de contrôle d'accès, la découverte automatique des données sensibles et l'exécution des tâches de découverte de données sensibles en cours.
- Macie annule toutes les tâches de découverte de données sensibles créées par le compte dans la région. Une tâche ne peut pas être reprise ou redémarrée après son annulation. Si vous avez créé des tâches pour analyser les données détenues par le compte du membre, Macie n'annule pas ces tâches. Au lieu de cela, les tâches ignorent les ressources détenues par le compte.

Lorsqu'un compte est suspendu, Macie conserve l'identifiant de session Macie, les paramètres et les ressources du compte dans la région applicable. Par exemple, les résultats du compte restent intacts et ne sont pas affectés pendant 90 jours au maximum. Le compte n'est pas débité pour l'utilisation de Macie dans la région applicable tant que Macie est suspendu pour le compte dans cette région.

Pour suspendre Macie pour un compte de membre dans une organisation basée sur des invitations

Pour suspendre Macie pour un compte membre dans une organisation basée sur des invitations, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie.

Console

Suivez ces étapes pour suspendre Macie pour un compte de membre à l'aide de la console Amazon Macie.

Pour suspendre Macie pour un compte de membre

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez suspendre Macie pour un compte de membre.
3. Dans le panneau de navigation, choisissez Accounts (Comptes). La page Comptes s'ouvre et affiche un tableau des comptes actuellement associés à votre compte.
4. Dans le tableau Comptes, cochez la case correspondant au compte que vous souhaitez suspendre.
5. Dans le menu Actions, choisissez Suspendre Macie.
6. Confirmez que vous souhaitez suspendre Macie pour le compte sélectionné.

Une fois que vous avez confirmé la suspension, le statut du compte passe à Suspendu (suspendu) dans l'inventaire de votre compte.

Répétez les étapes précédentes dans chaque région supplémentaire dans laquelle vous souhaitez suspendre Macie pour le compte.

API

Pour suspendre Macie pour un compte membre par programmation, utilisez l'API UpdateMemberSessionAmazon Macie. Lorsque vous soumettez votre demande, utilisez le `id` paramètre pour spécifier l'identifiant de compte à 12 chiffres du compte pour Compte AWS lequel vous souhaitez suspendre Macie. Pour le `status` paramètre, spécifiez `PAUSED` le nouveau statut du compte Macie. Spécifiez également la région à laquelle s'applique la demande. Pour suspendre Macie dans d'autres régions, soumettez votre demande dans chaque région supplémentaire.

Pour récupérer l'identifiant du compte membre, vous pouvez utiliser ListMembersl'API Amazon Macie. Dans ce cas, pensez à filtrer les résultats en incluant le `onlyAssociated` paramètre dans votre demande. Si vous définissez la valeur de ce paramètre sur`true`, Macie renvoie un `members` tableau qui fournit des détails uniquement sur les comptes actuellement membres de votre compte administrateur.

Pour suspendre Macie pour un compte de membre à l'aide de AWS CLI, exécutez la update-member-sessioncommande. Utilisez le `region` paramètre pour spécifier la région dans laquelle vous souhaitez suspendre Macie et utilisez le `id` paramètre pour spécifier l'ID du compte pour lequel vous souhaitez suspendre Macie. Pour le paramètre `status`, spécifiez `PAUSED`. Par exemple :

```
C:\> aws macie2 update-member-session --region us-east-1 --id 123456789012 --status
 PAUSED
```

Où *`us-east-1`* est la région dans laquelle Macie doit être suspendue (région des États-Unis de l'Est (Virginie du Nord)), 123456789012 est l'identifiant du compte pour lequel Macie doit être suspendu et le nouveau statut de Macie pour le compte. `PAUSED`

Si votre demande aboutit, Macie renvoie une réponse vide et le statut du compte spécifié est reporté `Paused` dans l'inventaire de votre compte.

Supprimer les comptes de membres Amazon Macie d'une organisation basée sur une invitation

En tant qu'administrateur Macie, vous pouvez supprimer un compte membre de votre organisation. Pour ce faire, dissociez le compte de votre compte administrateur Macie.

Si vous supprimez un compte de membre, Macie continue d'être activé pour ce compte et le compte continue d'apparaître dans l'inventaire de votre compte. Cependant, le compte devient un compte Macie autonome. Macie n'avertit pas le propriétaire du compte lorsque vous le supprimez. Par conséquent, pensez à contacter le propriétaire du compte pour vous assurer qu'il commence à gérer les paramètres et les ressources de son compte.

Lorsque vous supprimez un compte membre, vous perdez l'accès à tous les paramètres, ressources et données Macie du compte. Cela inclut les conclusions relatives aux politiques et les métadonnées relatives aux compartiments S3 détenus par le compte. En outre, vous ne pouvez plus utiliser Macie pour découvrir des données sensibles dans les compartiments S3 détenus par le compte. Si vous avez déjà créé des tâches de découverte de données sensibles à cette fin, les tâches ignorent les compartiments détenus par le compte. Si vous avez activé la découverte automatique des données sensibles pour le compte, vous et le compte perdez l'accès aux données statistiques, aux données d'inventaire et aux autres informations produites et fournies directement par Macie lors de la découverte automatique du compte.

Après avoir supprimé un compte membre, vous pouvez l'ajouter à nouveau à votre organisation en envoyant une nouvelle invitation au compte. Si le compte accepte la nouvelle invitation et que vous activez la découverte automatique des données sensibles pour le compte dans les 30 jours, vous retrouvez également l'accès aux données et informations que Macie avait précédemment produites et fournies directement lors de la découverte automatique du compte.

Si vous supprimez un compte de membre et que vous n'avez pas l'intention de l'ajouter à nouveau, vous pouvez le supprimer complètement de l'inventaire de votre compte. Pour savoir comment procéder, veuillez consulter la section Supprimer des associations avec d'autres comptes.

Pour supprimer un compte membre d'une organisation basée sur une invitation

Pour supprimer un compte membre de votre organisation, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie.

Console

Suivez ces étapes pour supprimer un compte membre à l'aide de la console Amazon Macie.

Pour supprimer un compte de membre

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez supprimer le compte membre.
3. Dans le panneau de navigation, choisissez Accounts (Comptes). La page Comptes s'ouvre et affiche un tableau des comptes actuellement associés à votre compte.
4. Dans le tableau Comptes, cochez la case correspondant au compte que vous souhaitez supprimer.
5. Dans le menu Actions, choisissez Dissocier le compte.
6. Confirmez que vous souhaitez supprimer le compte sélectionné en tant que compte membre.

Une fois que vous avez confirmé votre sélection, le statut du compte passe à Supprimé (dissocié) dans l'inventaire de votre compte.

Répétez les étapes précédentes dans chaque région supplémentaire dans laquelle vous souhaitez supprimer le compte de membre.

API

Pour supprimer un compte membre par programmation, utilisez l'DisassociateMemberAPI Amazon Macie. Lorsque vous soumettez votre demande, utilisez le `id` paramètre pour spécifier l' Compte AWS identifiant à 12 chiffres du compte membre à supprimer. Spécifiez également la région à laquelle s'applique la demande. Pour supprimer le compte dans d'autres régions, soumettez votre demande dans chaque région supplémentaire.

Pour récupérer l'identifiant du compte à supprimer, vous pouvez utiliser ListMembersl'API Amazon Macie. Dans ce cas, pensez à filtrer les résultats en incluant le `onlyAssociated` paramètre dans votre demande. Si vous définissez la valeur de ce paramètre sur`true`, Macie renvoie un `members` tableau qui fournit des détails uniquement sur les comptes actuellement membres de votre compte.

Pour supprimer un compte membre à l'aide de AWS CLI, exécutez la commande disassociate-member. Utilisez le `region` paramètre pour spécifier la région dans laquelle vous souhaitez supprimer le compte. Utilisez le `id` paramètre pour spécifier l'ID du compte à supprimer. Par exemple :

```
C:\> aws macie2 disassociate-member --region us-east-1 --id 123456789012
```

Où *us-east-1* est la région dans laquelle le compte doit être supprimé (région USA Est (Virginie du Nord)) *et* 123456789012 est l'identifiant du compte à supprimer.

Si votre demande aboutit, Macie renvoie une réponse vide et le statut du compte spécifié est reporté `Removed` dans l'inventaire de votre compte.

Supprimer des associations avec d'autres comptes

Après avoir ajouté un compte à l'inventaire de votre compte, vous pouvez supprimer l'association entre votre compte et l'autre compte. Vous pouvez le faire pour n'importe quel compte de votre inventaire, à l'exception des comptes suivants :

- Un compte qui fait partie de votre organisation dans AWS Organizations. Ce type d'association n'est AWS Organizations pas contrôlé par Macie.
- Un compte de membre qui a accepté une invitation d'adhésion de Macie à rejoindre votre organisation. Dans ce cas, vous devez supprimer le compte membre avant de pouvoir supprimer l'association.

Lorsque vous supprimez une association, Macie supprime le compte de l'inventaire de votre compte. Si vous souhaitez restaurer ultérieurement l'association, vous devez ajouter à nouveau le compte comme s'il s'agissait d'un tout nouveau compte.

Pour supprimer une association avec un autre compte

Pour supprimer une association entre votre compte et un autre compte, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie.

Console

Pour utiliser la console Amazon Macie afin de supprimer une association avec un autre compte, procédez comme suit.

Pour supprimer une association

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez supprimer l'association.
3. Dans le panneau de navigation, choisissez Accounts (Comptes). La page Comptes s'ouvre et affiche un tableau des comptes actuellement associés à votre compte.

4. Dans le tableau Comptes, cochez la case du compte dont vous souhaitez supprimer l'association.
5. Dans le menu Actions, sélectionnez Delete (Supprimer).
6. Confirmez que vous souhaitez supprimer l'association sélectionnée.

Répétez les étapes précédentes dans chaque région supplémentaire dans laquelle vous souhaitez supprimer l'association.

API

Pour supprimer une association avec un autre compte par programmation, utilisez l'DeleteMemberAPI Amazon Macie. Lorsque vous soumettez votre demande, utilisez le `id` paramètre pour spécifier l'identifiant de compte à 12 chiffres avec lequel Compte AWS vous souhaitez supprimer l'association. Spécifiez également la région à laquelle s'applique la demande. Pour supprimer l'association dans d'autres régions, soumettez votre demande dans chaque région supplémentaire.

Pour récupérer l'identifiant du compte, vous pouvez utiliser ListMembersl'API Amazon Macie. Dans ce cas, incluez le `onlyAssociated` paramètre dans votre demande et définissez la valeur du paramètre sur`false`. Si l'opération aboutit, Macie renvoie un `members` tableau qui fournit des détails sur tous les comptes associés à votre compte, y compris les comptes qui ne sont pas actuellement des comptes membres.

Pour supprimer une association avec un autre compte à l'aide de AWS CLI, exécutez la commande delete-member. Utilisez le `region` paramètre pour spécifier la région dans laquelle vous souhaitez supprimer l'association et le `id` paramètre pour spécifier l'ID de compte du compte. Par exemple :

```
C:\> aws macie2 delete-member --region us-east-1 --id 123456789012
```

Où *`us-east-1`* est la région dans laquelle supprimer l'association avec l'autre compte (la région USA Est (Virginie du Nord)) *`et`* 123456789012 est l'identifiant du compte.

Si votre demande aboutit, Macie renvoie une réponse vide et l'association entre votre compte et l'autre compte est supprimée. Le compte précédemment associé est supprimé de l'inventaire de votre compte.

Révision des comptes Amazon Macie pour une organisation basée sur des invitations

Pour vous aider à gérer les comptes de votre organisation, Amazon Macie fournit un inventaire des comptes associés à votre compte Macie dans chaque Région AWS endroit où vous utilisez Macie. En tant qu'administrateur Macie d'une organisation, vous pouvez utiliser cet inventaire pour consulter les statistiques et les informations relatives aux comptes de votre organisation. Vous pouvez également l'utiliser pour effectuer certaines tâches de gestion pour les comptes des membres et pour gérer le statut de la relation entre votre compte et les autres comptes.

Pour consulter les comptes d'une organisation basée sur des invitations

Pour consulter les comptes de votre organisation, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie.

Console

Suivez ces étapes pour consulter les comptes de votre organisation à l'aide de la console Amazon Macie.

Pour consulter les comptes de votre organisation

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez consulter les comptes de votre organisation.
3. Dans le panneau de navigation, choisissez Accounts (Comptes).

La page Comptes s'ouvre et affiche des statistiques agrégées ainsi qu'un tableau des comptes actuellement Région AWS associés à votre compte Macie.

En haut de la page Comptes, vous trouverez les statistiques agrégées suivantes.

Via AWS Organizations

Si vous êtes l'administrateur Macie d'une organisation dans AWS Organizations, Active indique le nombre total de comptes associés à votre compte par le biais de comptes membres Macie de votre organisation AWS Organizations et qui sont actuellement des comptes membres de Macie. Macie est activé pour ces comptes et vous êtes l'administrateur Macie des comptes.

All indique le nombre total de comptes associés à votre compte via AWS Organizations, y compris les comptes qui ne sont pas actuellement des comptes membres de Macie.

Sur invitation

Active indique le nombre total de comptes actuellement membres de Macie dans votre organisation basée sur des invitations. Macie est activé pour ces comptes et vous êtes l'administrateur Macie des comptes car ils ont accepté une invitation d'adhésion de votre part.

All indique le nombre total de comptes associés à votre compte par invitation Macie, y compris les comptes qui n'ont pas répondu à une invitation de votre part.

Actif/Tout

Active indique le nombre total de comptes actuellement membres de Macie pour votre compte, via AWS Organizations ou sur invitation. Macie est activé pour ces comptes et vous êtes l'administrateur Macie des comptes.

All indique le nombre total de comptes associés à votre compte, par le biais AWS Organizations ou sur invitation. Cela inclut les comptes qui n'ont pas accepté une invitation d'adhésion à Macie de votre part. Cela inclut également les comptes qui sont associés à votre compte par le biais de comptes Macie AWS Organizations et qui ne sont pas actuellement membres de Macie.

Dans le tableau, vous trouverez des informations sur chaque compte de la région actuelle. Le tableau inclut tous les comptes associés à votre compte Macie, que ce soit sur invitation ou via Macie. AWS Organizations

ID de compte

L'identifiant du compte et l'adresse e-mail du Compte AWS.

Nom

Le nom du compte pour Compte AWS. Cette valeur est généralement N/A pour les comptes associés à votre compte sur invitation.

Type

Comment le compte est associé à votre compte, sur invitation ou via AWS Organizations.

Statut

État de la relation entre votre compte et le compte. Pour un compte dans une organisation basée sur des invitations (Type is By invitation), les valeurs possibles sont les suivantes :

- Compte suspendu — Le compte Compte AWS est suspendu.
- Créé (invitation) — Vous avez ajouté le compte mais vous ne lui avez pas envoyé d'invitation d'adhésion.
- Échec de la vérification par e-mail : vous avez essayé d'envoyer une invitation d'adhésion au compte, mais l'adresse e-mail spécifiée n'est pas valide pour le compte.
- Vérification par e-mail en cours — Vous avez envoyé une invitation d'adhésion au compte et Macie traite la demande.
- Activé — Le compte est un compte de membre. Macie est activé pour le compte et vous êtes l'administrateur Macie du compte.
- Invité : vous avez envoyé une invitation d'adhésion au compte et celui-ci n'a pas répondu à votre invitation.
- Démission du membre — Le compte était auparavant un compte membre. Cependant, le compte a quitté votre organisation en se dissociant de votre compte.
- Suspendu (suspendu) — Le compte est un compte de membre, mais Macie est actuellement suspendu pour le compte.
- Région désactivée — La région actuelle est désactivée pour le Compte AWS.
- Supprimé (dissocié) — Le compte était auparavant un compte de membre. Cependant, vous l'avez supprimé en tant que compte membre en le dissociant de votre compte.

Dernière mise à jour du statut

Lorsque vous ou le compte associé avez récemment effectué une action qui a eu une incidence sur la relation entre vos comptes.

Découverte automatisée des données sensibles

Si la découverte automatique des données sensibles est actuellement activée ou désactivée pour le compte.

Pour trier le tableau en fonction d'un champ spécifique, choisissez l'en-tête de colonne du champ. Pour modifier l'ordre de tri, choisissez à nouveau l'en-tête de colonne. Pour filtrer le tableau, placez votre curseur dans la zone de filtre, puis ajoutez une condition de filtre pour un

champ. Pour affiner davantage les résultats, ajoutez des conditions de filtre pour des champs supplémentaires.

API

Pour consulter les comptes de votre organisation par programmation, utilisez l'ListMembersAPI Amazon Macie et spécifiez la région à laquelle s'applique votre demande. Pour consulter les détails dans d'autres régions, soumettez votre demande dans chaque région supplémentaire.

Lorsque vous soumettez votre demande, utilisez le `onlyAssociated` paramètre pour spécifier les comptes à inclure dans la réponse. Par défaut, Macie renvoie uniquement les informations relatives aux comptes membres de la région spécifiée, sur invitation ou via AWS Organizations. Pour récupérer les détails de tous les comptes associés, y compris les comptes qui ne sont pas des comptes membres, incluez le `onlyAssociated` paramètre dans votre demande et définissez la valeur du paramètre sur`false`.

Pour consulter les comptes de votre organisation à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande list-members. Pour le `only-associated` paramètre, spécifiez si vous souhaitez inclure tous les comptes associés ou uniquement les comptes des membres. Pour inclure uniquement les comptes des membres, omettez ce paramètre ou définissez la valeur du paramètre sur`true`. Pour inclure tous les comptes, définissez cette valeur sur`false`. Par exemple :

```
C:\> aws macie2 list-members --region us-east-1 --only-associated false
```

Où *`us-east-1`* est la région à laquelle s'applique la demande, la région USA Est (Virginie du Nord).

Si votre demande aboutit, Macie renvoie un `members` tableau. Le tableau contient un `member` objet pour chaque compte qui répond aux critères spécifiés dans la demande. Dans cet objet, le `relationshipStatus` champ indique le statut actuel de l'association entre votre compte et l'autre compte dans la région spécifiée. Pour un compte dans une organisation basée sur des invitations, les valeurs possibles sont les suivantes :

- `AccountSuspended`— Le Compte AWS est suspendu.
- `Created`— Vous avez ajouté le compte mais vous ne lui avez pas envoyé d'invitation d'adhésion.
- `EmailVerificationFailed`— Vous avez essayé d'envoyer une invitation d'adhésion au compte, mais l'adresse e-mail spécifiée n'est pas valide pour le compte.

- `EmailVerificationInProgress`— Vous avez envoyé une invitation d'adhésion au compte et Macie traite la demande.
- `Enabled`— Le compte est un compte de membre. Macie est activé pour le compte et vous êtes l'administrateur Macie du compte.
- `Invited`— Vous avez envoyé une invitation d'adhésion au compte et celui-ci n'a pas répondu à votre invitation.
- `Paused`— Le compte est un compte de membre mais Macie est actuellement suspendu (suspendu) pour le compte.
- `RegionDisabled`— La région actuelle est désactivée pour le Compte AWS.
- `Removed`— Le compte était auparavant un compte de membre. Cependant, vous l'avez supprimé en tant que compte membre en le dissociant de votre compte.
- `Resigned`— Le compte était auparavant un compte de membre. Cependant, le compte a quitté votre organisation en se dissociant de votre compte.

Pour plus d'informations sur les autres champs de l'`member`objet, consultez la section Membres du manuel Amazon Macie API Reference.

Désignation d'un compte administrateur Amazon Macie différent pour une organisation basée sur des invitations

Après avoir créé et établi une organisation basée sur des invitations, vous pouvez modifier le compte administrateur Amazon Macie de l'organisation. Pour ce faire, les administrateurs et les membres de l'organisation doivent suivre les étapes suivantes :

1. L'administrateur Macie actuel exporte éventuellement l'inventaire actuel des comptes de membres actifs de l'organisation. Cela simplifie la transition en vous aidant à identifier les comptes de membres qui devraient continuer à faire partie de l'organisation.
2. L'administrateur Macie actuel supprime tous les comptes membres de l'organisation actuelle. Cela dissocie les comptes du compte administrateur actuel. Macie continue d'être activé pour les comptes, mais les comptes deviennent des comptes Macie autonomes.

> **Note**
>
> Lorsque l'administrateur Macie actuel supprime les comptes des membres, Macie désactive automatiquement la découverte automatique des données sensibles pour

les comptes. Cela désactive également l'accès aux données statistiques, aux données d'inventaire et aux autres informations produites et fournies directement par Macie lors de la découverte automatique des comptes. Lorsque la transition vers la nouvelle organisation est terminée, le nouvel administrateur Macie ne peut pas accéder à ces données.

3. Le nouvel administrateur Macie ajoute les comptes des membres précédents à la nouvelle organisation. Cela permet d'associer les comptes au nouveau compte administrateur.
4. Chaque compte membre accepte l'invitation à rejoindre la nouvelle organisation. Lorsqu'un compte accepte l'invitation, il devient un compte de membre actif dans la nouvelle organisation. Le nouvel administrateur Macie peut alors accéder aux paramètres, aux données et aux ressources Macie du compte. Si la découverte automatique des données sensibles a déjà été activée pour le compte, cela n'inclut pas les données que Macie a précédemment produites et fournies directement lors de la découverte automatique du compte. Macie génère et gère plutôt de nouvelles données pour le compte, si le nouvel administrateur Macie active la découverte automatique du compte.

Si votre organisation utilise Macie à plusieurs reprises Régions AWS, effectuez les étapes précédentes dans chacune de ces régions.

Pour exporter l'inventaire actuel des comptes de membres actifs, l'administrateur Macie actuel peut utiliser la console Amazon Macie ou l'API Amazon Macie. Avec la console, l'administrateur actuel peut exporter les données vers un fichier de valeurs séparées par des virgules (CSV). Le nouvel administrateur peut ensuite utiliser la console pour télécharger le fichier CSV et ajouter tous les comptes (en bloc) à la nouvelle organisation.

Pour exporter les données du compte d'un membre à l'aide de la console

1. Connectez-vous à l' AWS Management Console aide du compte administrateur Macie actuel.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez exporter les données.
3. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
4. Dans le panneau de navigation, choisissez Accounts (Comptes). La page Comptes s'ouvre et affiche un tableau des comptes associés au compte administrateur Macie actuel.
5. (Facultatif) Pour filtrer le tableau des comptes et n'afficher que les comptes qui sont actuellement des comptes membres Macie actifs dans l'organisation, utilisez le champ de filtre situé au-dessus du tableau pour ajouter les conditions de filtre suivantes :

   - Type = Invitation

- État = Activé

6. Dans le tableau Comptes, cochez la case correspondant à chaque compte membre à inclure dans les données exportées.
7. Choisissez Exporter au format CSV.
8. Spécifiez le nom et l'emplacement du fichier.

Avec l'API Amazon Macie, l'administrateur Macie actuel peut récupérer les données au format JSON. Le nouvel administrateur Macie peut ensuite utiliser ces données pour générer la liste des identifiants de compte et des adresses e-mail pour les comptes à ajouter et à inviter à rejoindre la nouvelle organisation. Pour récupérer les données au format JSON, utilisez le ListMembersfonctionnement de l'API Amazon Macie. Si l'opération aboutit, Macie renvoie un `members` tableau fournissant des détails sur tous les comptes associés au compte de l'administrateur. Si un compte est un compte de membre Macie actif dans l'organisation actuelle basée sur des invitations, la valeur de la `relationshipStatus` propriété du compte est `Enabled` et la `invitedAt` propriété spécifie une date et une heure.

Gérer votre adhésion à une organisation basée sur des invitations dans Amazon Macie

Si vous êtes invité à rejoindre une organisation sur Amazon Macie, vous pouvez éventuellement accepter ou refuser l'invitation. Dans Macie, une organisation est un ensemble de comptes gérés de manière centralisée en tant que groupe de comptes connexes. Une organisation se compose d'un compte administrateur Macie désigné et d'un ou plusieurs comptes de membres associés.

Si vous acceptez une invitation, votre compte devient un compte membre de l'organisation. Lorsque vous acceptez, le compte qui a envoyé l'invitation devient le compte administrateur Macie de votre compte : vous associez votre compte à l'autre compte et vous activez une relation administrateur-membre entre les comptes. Le compte administrateur Macie peut ensuite accéder à certains paramètres, données et ressources Macie pour votre compte dans le cas applicable. Région AWS Pour plus d'informations, consultez Comprendre la relation entre les comptes d'administrateur et de membre d'Amazon Macie.

Si vous refusez une invitation, le statut actuel et les paramètres de votre compte Macie ne sont pas modifiés.

Rubriques

- Répondre aux invitations d'adhésion adressées aux organisations
- Dissociation d'un compte administrateur Amazon Macie

Répondre aux invitations d'adhésion adressées aux organisations

Lorsque vous recevez une invitation à rejoindre une organisation, Amazon Macie vous en informe de plusieurs manières. Par défaut, Macie vous envoie l'invitation sous forme de message électronique. Macie crée également un AWS Health événement pour votre Compte AWS. Si vous utilisez déjà Macie à Région AWS partir duquel l'invitation a été envoyée, Macie affiche également un badge Accounts et une notification sur la console Macie.

Après avoir reçu une invitation, vous pouvez éventuellement l'accepter ou la refuser. Avant de répondre, notez ce qui suit :

- Vous ne pouvez être membre que d'une seule organisation à la fois. Si vous recevez plusieurs invitations, vous ne pouvez en accepter qu'une seule. Ou, si vous êtes déjà membre d'une organisation, vous devez dissocier votre compte de son compte administrateur Macie actuel avant de pouvoir rejoindre une autre organisation.
- Si vous utilisez Macie dans plusieurs régions, votre compte doit avoir le même compte administrateur Macie dans toutes ces régions. L'administrateur Macie doit vous envoyer des invitations séparément pour chaque région, et vous devez accepter les invitations séparément dans chaque région.
- Pour accepter ou refuser une invitation, vous devez activer Macie dans la région d'où l'invitation a été envoyée. Le refus d'une invitation est facultatif. Si vous autorisez Macie à refuser une invitation, vous pouvez désactiver Macie dans la région après avoir décliné l'invitation. Cela vous permet de ne pas encourir de frais inutiles pour utiliser Macie dans la région.
- Si la découverte automatique des données sensibles est activée pour votre compte et que vous acceptez une invitation, vous perdez l'accès aux données statistiques, aux données d'inventaire et aux autres informations produites et fournies directement par Macie lors de la découverte automatique de votre compte. Une fois que vous avez accepté une invitation, votre administrateur Macie peut activer la découverte automatique de votre compte. Toutefois, cela ne rétablit pas l'accès aux données existantes. Au lieu de cela, Macie génère et gère de nouvelles données tout en effectuant la découverte automatique de votre compte.

Pour des considérations supplémentaires, voirRépondre aux invitations aux membres et les gérer.

Pour répondre à une invitation à devenir membre d'une organisation

Pour répondre à une invitation d'adhésion, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie.

Console

Suivez ces étapes pour répondre à une invitation d'adhésion à l'aide de la console Amazon Macie.

Pour répondre à une invitation d'adhésion

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous avez reçu l'invitation.
3. Si vous n'avez pas activé Macie dans la région, choisissez Commencer, puis sélectionnez Activer Macie. Vous devez activer Macie avant de pouvoir accepter ou refuser une invitation.
4. Dans le panneau de navigation, choisissez Accounts (Comptes).
5. Sous Compte administrateur, effectuez l'une des opérations suivantes :

   - Pour accepter l'invitation, activez Accepter
     ( )
     à côté de l'invitation. Choisissez ensuite Accepter l'invitation ou Mettre à jour, selon que vous avez déjà accepté une autre invitation.
   - Pour refuser l'invitation, choisissez Refuser l'invitation à côté de l'invitation, puis confirmez que vous souhaitez refuser l'invitation.

Si vous avez reçu l'invitation et souhaitez y répondre dans d'autres régions, répétez les étapes précédentes dans chaque région supplémentaire.

API

Pour répondre à une invitation par programmation, utilisez l'API Amazon DeclineInvitationsMacie AcceptInvitationou utilisez l'API Amazon Macie, selon que vous souhaitez accepter ou refuser l'invitation. Lorsque vous soumettez votre demande, assurez-vous de spécifier la région depuis laquelle l'invitation a été envoyée. Pour répondre à l'invitation dans d'autres régions, soumettez votre demande dans chaque région supplémentaire.

Dans une `AcceptInvitation` demande, utilisez le `administratorAccountId` paramètre pour spécifier l'identifiant de compte à 12 chiffres de l' Compte AWS expéditeur de l'invitation. Utilisez le `invitationId` paramètre pour spécifier l'identifiant unique de l'invitation à accepter.

Dans une `DeclineInvitations` demande, utilisez le `accountIds` paramètre pour spécifier l'identifiant de compte à 12 chiffres du compte Compte AWS qui a envoyé l'invitation à refuser.

Pour récupérer les identifiants, vous pouvez utiliser le ListInvitationsfonctionnement de l'API Amazon Macie. Si l'opération aboutit, Macie renvoie un `invitations` tableau fournissant des détails sur les invitations que vous avez reçues, y compris l'identifiant du compte qui a envoyé chaque invitation et l'identifiant unique de chaque invitation. Si la valeur de la `relationshipStatus` propriété d'une invitation est`Invited`, vous n'avez pas encore répondu à l'invitation.

Pour répondre à une invitation à l'aide de AWS Command Line Interface (AWS CLI), exécutez la commande accept-invitation ou decline-invitations, selon que vous souhaitez accepter ou refuser l'invitation. Utilisez le `region` paramètre pour spécifier la région depuis laquelle l'invitation a été envoyée. Par exemple :

```
C:\> aws macie2 accept-invitation --region us-east-1 --administrator-account-
id 123456789012 --invitation-id d8bdad0e203fd1242e0a4721bexample
```

Où *`us-east-1`* est la région d'où l'invitation a été envoyée (région USA Est (Virginie du Nord))*`,`* 123456789012 est l'identifiant du compte qui a envoyé l'invitation *`et`* d8bdad0e203fd1242e0a4721bexample est l'identifiant unique de l'invitation à accepter.

Si une demande d'acceptation d'une invitation aboutit, Macie renvoie une réponse vide. Si une demande de refus d'une invitation aboutit, Macie renvoie un tableau vide. `unprocessedAccounts`

Une fois que vous avez refusé une invitation, celle-ci est conservée en tant que ressource pour votre compte Macie. Vous pouvez éventuellement le supprimer en utilisant l'DeleteInvitationsopération ou, pour le AWS CLI, la commande delete-invitations.

Dissociation d'un compte administrateur Amazon Macie

Si vous acceptez une invitation à rejoindre une organisation sur Amazon Macie, vous pouvez ensuite démissionner de l'organisation en dissociant votre compte de son compte administrateur Macie actuel. Notez que vous ne pouvez pas le faire si votre compte est un compte membre d'une AWS Organizations organisation. Pour démissionner d'une AWS Organizations organisation, contactez votre administrateur Macie pour supprimer votre compte en tant que compte membre Macie.

Si vous dissociez votre compte de son compte administrateur Macie, l'administrateur Macie perd l'accès à tous les paramètres, données et ressources de votre compte Macie. Cela inclut les métadonnées et les conclusions relatives aux politiques relatives aux données Amazon S3 dont vous êtes propriétaire. Cela signifie également que l'administrateur ne peut plus analyser vos données Amazon S3 en effectuant une découverte automatique de données sensibles ou en exécutant des tâches de découverte de données sensibles.

Lorsque vous dissociez votre compte, Macie continue d'être activé pour votre compte dans la région applicable. Toutefois, votre compte devient un compte Macie autonome dans la Région. Le statut de votre compte passe à Membre démissionné dans l'inventaire des comptes de l'administrateur.

Pour se dissocier d'un compte administrateur Macie

Pour dissocier votre compte de son compte administrateur Macie actuel, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie.

Console

Suivez ces étapes pour dissocier votre compte de son compte administrateur Macie à l'aide de la console Amazon Macie.

Pour se dissocier d'un compte administrateur

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. À l'aide du Région AWS sélecteur situé dans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez dissocier votre compte de son compte administrateur.
3. Dans le panneau de navigation, choisissez Accounts (Comptes).
4. Sous Compte administrateur, désactivez Accepter () à côté de l'invitation, puis choisissez Mettre à jour.

Le compte continue d'apparaître sur la page Comptes. Si vous décidez de rejoindre à nouveau l'organisation, vous pouvez utiliser cette page pour accepter à nouveau l'invitation initiale. Vous pouvez également refuser et supprimer l'invitation, ce qui supprime également l'association entre votre compte et l'autre compte. Pour ce faire, choisissez Refuser l'invitation.

Si vous souhaitez dissocier votre compte de son compte administrateur Macie dans d'autres régions, répétez les étapes précédentes dans chaque région supplémentaire.

API

Pour dissocier votre compte de son compte administrateur Macie par programmation, utilisez l'API Amazon DisassociateFromAdministratorAccountMacie. Lorsque vous soumettez votre demande, assurez-vous de préciser la région à laquelle elle s'applique. Pour vous dissocier du compte dans d'autres régions, soumettez votre demande dans chaque région supplémentaire.

Pour dissocier votre compte de son compte administrateur Macie à l'aide de AWS CLI, exécutez la disassociate-from-administrator-accountcommande. Utilisez le `region` paramètre pour spécifier la région dans laquelle vous souhaitez vous dissocier du compte.

Si votre demande aboutit, Macie renvoie une réponse vide.

Une fois que vous vous êtes dissocié du compte, l'invitation d'origine est conservée en tant que ressource pour votre compte Macie, sauf si vous la supprimez. Si vous décidez de rejoindre à nouveau l'organisation, vous pouvez utiliser cette ressource pour accepter à nouveau l'invitation initiale. Vous pouvez également supprimer l'invitation en utilisant l'DeleteInvitationsopération ou, dans le cas de la AWS CLI, la commande delete-invitations. Si vous supprimez l'invitation, vous supprimez également l'association entre votre compte et l'autre compte.

Amazon Macie

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre 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 exécute des Services AWS dans le AWS Cloud. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des AWS programmes de conformité. Pour en savoir Amazon Macie sur lesAWS programmes
- Sécurité dans le cloud – Votre responsabilité est fonction du Services AWS 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.

Amazon Les rubriques suivantes Amazon AmazonServices AWS

Rubriques

- Protection des données dans Amazon Macie
- Gestion des identités et des accès pour Amazon Macie
- Journalisation et surveillance dans Amazon Macie
- Validation de conformité pour Amazon Macie
- Résilience dans Amazon Macie
- Sécurité de l'infrastructure dans Amazon Macie
- Amazon Macie et points de terminaison VPC d'interface () AWS PrivateLink

Protection des données dans Amazon Macie

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon Macie. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure globale sur laquelle l'ensemble d'AWS Cloud s'exécute. 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 pour les Services AWS que vous utilisez. Pour en savoir plus 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 AWSet RGPD (Règlement général sur la protection des données) sur le AWSBlog de sécurité.

À des fins de protection des données, nous vous recommandons de protéger les informations d'identification Compte AWS et de configurer les comptes utilisateur 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 les certificats SSL/TLS pour communiquer avec les ressources AWS. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez une API (Interface de programmation) et le journal de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de chiffrement AWS, ainsi que tous les contrôles de sécurité par défaut au sein des 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 FIPS (Federal Information Processing Standard) 140-2 lorsque vous accédez à AWS via une CLI (Interface de ligne de commande) ou une API (Interface de programmation), utilisez un point de terminaison FIPS (Federal Information Processing Standard). Pour en savoir plus 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 Macie ou une autre personne à Services AWS l'aide de la console, de l'API ou des AWS SDK. AWS CLI Toutes les données que vous saisissez 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.

Chiffrement au repos

Amazon Macie stocke vos données au repos en toute sécurité à l'aide de solutions de AWS chiffrement. Macie chiffre les données, telles que les résultats, à l'aide d'un Clé gérée par AWS from AWS Key Management Service ()AWS KMS.

Si vous désactivez Macie, il supprime définitivement toutes les ressources qu'il stocke ou gère pour vous, telles que les tâches de découverte de données sensibles, les identifiants de données personnalisés et les résultats.

Chiffrement en transit

Macie chiffre toutes les données en transit entre les deux. Services AWS

Amazon Macie analyse les données d'Amazon S3 et exporte les résultats de découverte de données sensibles vers un compartiment S3. Une fois que Macie a obtenu les informations dont il a besoin à partir des objets S3, ils sont supprimés.

Macie accède à Amazon S3 via un point de terminaison VPC alimenté par. AWS PrivateLink Par conséquent, le trafic entre Macie et Amazon S3 reste sur le réseau Amazon et ne passe pas par l'Internet public. Pour plus d'informations, consultez AWS PrivateLink.

Gestion des identités et des accès pour Amazon Macie

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 qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources Macie. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Rôles liés à un service pour Amazon Macie
- AWSpolitiques gérées pour Amazon Macie
- Résolution des problèmes d'identité et d'accès à Amazon Macie

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Macie.

Utilisateur du service : si vous utilisez le service Macie pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités de Macie pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne parvenez pas à accéder à une fonctionnalité dans Macie, consultezRésolution des problèmes d'identité et d'accès à Amazon Macie.

Administrateur du service — Si vous êtes responsable des ressources Macie dans votre entreprise, vous avez probablement un accès complet à Macie. C'est à vous de déterminer les fonctionnalités et ressources Macie auxquelles les utilisateurs de votre service doivent 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 Macie, consultez. Comment fonctionne Amazon Macie avec AWS Identity and Access Management

Administrateur IAM — Si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Macie. Pour consulter des exemples de politiques basées sur l'identité Macie que vous pouvez utiliser dans IAM, consultez. Exemples de stratégies basées sur l'identité pour Amazon Macie

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 fonctionne Amazon Macie avec AWS Identity and Access Management

Avant d'utiliser AWS Identity and Access Management (IAM) pour gérer l'accès à Amazon Macie, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Macie.

Fonctionnalités IAM que vous pouvez utiliser avec Amazon Macie

Fonction IAM	Support Macie
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non

Fonction IAM	Support Macie
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d'une politique	Oui
Listes de contrôle d'accès (ACL)	Non
Contrôle d'accès basé sur les attributs (ABAC) : balises 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 une présentation détaillée de la façon dont Macie et d'autres utilisent la Services AWS plupart des fonctionnalités IAM, consultez le guide de l'Services AWS utilisateur IAM consacré à l'utilisation d'IAM.

Politiques basées sur l'identité pour Amazon Macie

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.

Macie soutient les politiques basées sur l'identité. Pour obtenir des exemples, consultez Exemples de stratégies basées sur l'identité pour Amazon Macie.

Politiques basées sur les ressources au sein d'Amazon Macie

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.

Macie ne prend pas en charge les politiques basées sur les ressources. En d'autres termes, vous ne pouvez pas associer une politique directement à une ressource Macie.

Actions politiques pour Amazon Macie

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.

Les actions politiques pour Macie utilisent le préfixe suivant avant l'action :

```
macie2
```

Par exemple, pour autoriser quelqu'un à accéder aux informations relatives à tous les identifiants de données gérés fournis par Macie, action correspondant au `ListManagedDataIdentifiers` fonctionnement de l'API Amazon Macie, incluez `macie2:ListManagedDataIdentifiers` l'action dans sa politique :

```
"Action": "macie2:ListManagedDataIdentifiers"
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules. Par exemple :

```
"Action": [
      "macie2:ListManagedDataIdentifiers",
      "macie2:ListCustomDataIdentifiers"
]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `List`, incluez l'action suivante :

```
"Action": "macie2:List*"
```

Cependant, une bonne pratique consiste à créer des stratégies qui suivent le principe du moindre privilège. En d'autres termes, vous devez créer des stratégies qui incluent uniquement les autorisations requises pour effectuer une tâche spécifique.

Pour obtenir la liste des actions Macie, consultez la section Actions définies par Amazon Macie dans le Service Authorization Reference. Pour des exemples de politiques qui spécifient les actions Macie, voirExemples de stratégies basées sur l'identité pour Amazon Macie.

Ressources relatives aux politiques pour Amazon Macie

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": "*"
```

Macie définit les types de ressources suivants :

- Liste verte

- Identifiant de données personnalisé
- Règle de filtrage ou de suppression, également appelée filtre de résultats
- Compte membre
- Tâche de découverte de données sensibles, également appelée tâche de classification

Vous pouvez spécifier ces types de ressources dans les politiques à l'aide des ARN.

Par exemple, pour créer une politique pour la tâche de découverte de données sensibles portant l'ID de tâche 3ce05dbb7ec5505def334104bexample, vous pouvez utiliser l'ARN suivant :

```
"Resource": "arn:aws:macie2:*:*:classification-job/3ce05dbb7ec5505def334104bexample"
```

Ou, pour spécifier toutes les tâches de découverte de données sensibles pour un compte donné, utilisez un caractère générique (*) :

```
"Resource": "arn:aws:macie2:*:123456789012:classification-job/*"
```

Où *123456789012* est l'identifiant du compte qui a créé les Compte AWS emplois. En tant que bonne pratique, vous devez toutefois créer des politiques qui respectent le principe du moindre privilège. En d'autres termes, vous devez créer des politiques qui incluent uniquement les autorisations requises pour effectuer une tâche spécifique sur une ressource spécifique.

Certaines actions Macie peuvent s'appliquer à plusieurs ressources. Par exemple, l'`macie2:BatchGetCustomDataIdentifiers`action peut récupérer les détails de plusieurs identifiants de données personnalisés. Dans ces cas, le principal doit être autorisé à accéder à toutes les ressources auxquelles s'applique l'action. Pour spécifier plusieurs ressources dans une seule instruction, séparez les ARN par des virgules.

```
"Resource": [
 "arn:aws:macie2:*:*:custom-data-identifier/12g4aff9-8e22-4f2b-b3fd-3063eexample",
 "arn:aws:macie2:*:*:custom-data-identifier/2d12c96a-8e78-4ca6-b1dc-8fd65example",
 "arn:aws:macie2:*:*:custom-data-identifier/4383a69d-4a1e-4a07-8715-208ddexample"
]
```

Pour obtenir la liste des types de ressources Macie et la syntaxe ARN de chacun d'entre eux, consultez la section Types de ressources définis par Amazon Macie dans le Service Authorization Reference. Pour savoir quelles actions vous pouvez spécifier pour chaque type de ressource,

consultez la section Actions définies par Amazon Macie dans la référence d'autorisation de service. Pour des exemples de politiques qui spécifient les ressources, voirExemples de stratégies basées sur l'identité pour Amazon Macie.

Clés de conditions générales pour Amazon Macie

Prend en charge les clés de condition de politique spécifiques au service	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 `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.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. 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.

Pour obtenir la liste des clés de condition Macie, consultez la section Clés de condition pour Amazon Macie dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par Amazon Macie.

Pour des exemples de politiques utilisant des clés de condition, consultezExemples de stratégies basées sur l'identité pour Amazon Macie.

Listes de contrôle d'accès (ACL) dans Amazon Macie

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.

Amazon Simple Storage Service (Amazon S3) en est un exemple qui prend en charge les Service AWS ACL. Pour en savoir plus, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Macie ne prend pas en charge les ACL. C'est-à-dire que vous ne pouvez pas associer une ACL à une ressource Macie.

Contrôle d'accès basé sur les attributs (ABAC) avec Amazon Macie

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.

Vous pouvez associer des balises aux ressources Macie : listes d'autorisation, identifiants de données personnalisés, règles de filtrage et règles de suppression, comptes membres et tâches de découverte de données sensibles. Vous pouvez également contrôler l'accès à ces types de ressources en fournissant des informations de balise dans l'`Condition`élément d'une politique. Pour plus d'informations sur le balisage des ressources Macie, consultez. Marquage des ressources Amazon Macie Pour un exemple de politique basée sur l'identité qui contrôle l'accès à une ressource en fonction de balises, consultez. Exemples de stratégies basées sur l'identité pour Amazon Macie

Utilisation d'informations d'identification temporaires avec Amazon Macie

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.

Macie prend en charge l'utilisation d'informations d'identification temporaires.

Transférer les sessions d'accès pour Amazon Macie

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.

Macie envoie des requêtes FAS en aval Services AWS lorsque vous effectuez les tâches suivantes :

- Créez ou mettez à jour les paramètres Macie pour une liste d'autorisations stockée dans un compartiment S3.
- Vérifiez l'état d'une liste d'autorisations stockée dans un compartiment S3.
- Récupérez des échantillons de données sensibles à partir d'un objet S3 concerné à l'aide des informations d'identification de l'utilisateur IAM.
- Chiffrez les échantillons de données sensibles extraits à l'aide des informations d'identification de l'utilisateur IAM ou d'un rôle IAM.
- Permettez à Macie de s'intégrer à AWS Organizations.
- Désignez le compte administrateur Macie délégué pour une organisation dans AWS Organizations.

Pour les autres tâches, Macie utilise un rôle lié à un service pour effectuer des actions en votre nom. Pour plus de détails sur ce rôle, consultezRôles liés à un service pour Amazon Macie.

Rôles de service pour Amazon Macie

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.

Macie n'assume ni n'utilise de rôles de service. Pour effectuer des actions en votre nom, Macie utilise principalement un rôle lié à un service. Pour plus de détails sur ce rôle, consultezRôles liés à un service pour Amazon Macie.

Rôles liés à un service pour Amazon Macie

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.

Macie utilise un rôle lié à un service pour effectuer des actions en votre nom. Pour plus de détails sur ce rôle, consultezRôles liés à un service pour Amazon Macie.

Exemples de stratégies basées sur l'identité pour Amazon Macie

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier des ressources Macie Ils ne peuvent pas non plus exécuter des tâches à l'aide de la AWS Management Console, de l'AWS Command Line Interface (AWS CLI) ou de l'API AWS. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM doit 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 Macie, y compris le format des ARN pour chacun des types de ressources, consultez Actions, ressources et clés de condition pour Amazon Macie

Lorsque vous créez une stratégie, veillez à résoudre les avertissements de sécurité, les erreurs, les avertissements généraux et les suggestions provenant d'AWS Identity and Access Management Access Analyzer(IAM Access Analyzer) avant d'enregistrer la stratégie IAM Access Analyzer exécute des vérifications de stratégies pour valider une stratégie par rapport à la grammaire de stratégie et aux bonnes pratiques IAM Ces vérifications génèrent des résultats et fournissent des recommandations exploitables pour vous aider à créer des stratégies fonctionnelles et conformes aux bonnes pratiques en matière de sécurité. Pour en savoir plus sur la validation des stratégies à l'aide d'IAM Access Analyzer, consultez Validation de stratégie IAM Access Analyzer dans le Guide de l'utilisateur IAM Pour afficher la liste des avertissements, erreurs et suggestions qu'IAM Access Analyzer peut renvoyer, consultez la Référence de vérification de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM

Rubriques

Bonnes pratiques en matière de politiques

Les stratégies basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources Macie 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 :

- Démarrer avec AWS gérées et évoluez vers les autorisations de moindre privilège - Pour commencer à accorder des autorisations à vos utilisateurs et charges de travail, utilisez les politiques gérées AWS qui accordent des autorisations dans de nombreux cas d'utilisation

courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire encore les autorisations en définissant des Politiques gérées par le client AWS qui sont spécifiques à vos cas d'utilisation. Pour de plus amples informations, consultez Politiques gérées AWS ou Politiques gérées 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 via un Service AWS spécifique, comme 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 de plus amples informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Authentification multifactorielle (MFA) nécessaire : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root dans votre Compte AWS, activez l'authentification multifactorielle pour une sécurité renforcée. Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour de plus amples 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.

Utilisation de la console Amazon Macie

Pour accéder à la console Amazon Macie Ces autorisations doivent vous permettre de répertorier et de consulter les détails concernant les ressources Macie Compte AWS Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Vous n'avez pas besoin d'accorder les autorisations minimales de console pour les utilisateurs qui effectuent des appels uniquement à AWS CLI ou à l'API AWS. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent utiliser la console Amazon Macie, créez des politiques IAM qui leur fournissent un accès à la console. Pour de plus amples informations, veuillez consulter Policies and permissions in IAM (Stratégies et autorisations dans IAM) dans le IAM Guide de l'utilisateur.

Si vous créez une politique qui autorise les utilisateurs ou les rôles à utiliser la console Amazon Macie, assurez-vous que la politique autorise l'`macie2:GetMacieSession`action. Dans le cas contraire, ces utilisateurs ou rôles ne pourront accéder à aucune ressource ou donnée Macie sur la console.

Assurez-vous également que la politique autorise les `macie2:List` actions appropriées pour les ressources auxquelles ces utilisateurs ou rôles doivent accéder sur la console. Dans le cas contraire, ils ne pourront pas accéder à ces ressources ni en afficher les détails sur la console. Par exemple, pour consulter les détails d'une tâche de découverte de données sensibles à l'aide de la console, un utilisateur doit être autorisé à effectuer l'`macie2:DescribeClassificationJob`action correspondant à la tâche et à l'`macie2:ListClassificationJobs`action. Si un utilisateur n'est pas autorisé à effectuer l'**`macie2:ListClassificationJobs`**action, il ne pourra pas afficher la liste des tâches sur la page Tâches de la console et ne pourra donc pas choisir la tâche pour en afficher les détails. Pour que les détails incluent des informations sur un identifiant de données personnalisé utilisé par la tâche, l'utilisateur doit également être autorisé à effectuer l'`macie2:BatchGetCustomDataIdentifiers`action correspondant à l'identifiant de données personnalisé.

Exemple : autoriser des utilisateurs à modifier 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 nécessaires pour réaliser cette action sur la console ou par programmation à l'aide de l'AWS CLI ou de l'API 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": "*"
        }
    ]
}
```

Exemple : autoriser les utilisateurs à créer des tâches de découverte de données sensibles

Cet exemple montre comment créer une stratégie qui autorise un utilisateur à créer des tâches de découverte de données sensibles

Dans l'exemple, la première instruction accorde des `macie2:CreateClassificationJob` autorisations à l'utilisateur. Ces autorisations permettent à l'utilisateur de créer des tâches. La déclaration accorde également des `macie2:DescribeClassificationJob` autorisations. Ces autorisations permettent à l'utilisateur d'accéder aux détails des tâches existantes. Bien que ces autorisations ne soient pas requises pour créer des tâches, l'accès à ces informations peut aider l'utilisateur à créer des tâches dotées de paramètres de configuration uniques.

La deuxième instruction de l'exemple permet à l'utilisateur de créer, de configurer et de réviser des tâches à l'aide de la console Amazon Macie. Les `macie2:ListClassificationJobs` autorisations permettent à l'utilisateur d'afficher les tâches existantes sur la page Tâches de la console. Toutes les autres autorisations de l'instruction permettent à l'utilisateur de configurer et de créer une tâche à l'aide des pages Créer une tâche sur la console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndReviewJobs",
            "Effect": "Allow",
            "Action": [
                "macie2:CreateClassificationJob",
                "macie2:DescribeClassificationJob"
            ],
            "Resource": "arn:aws:macie2:*:*:classification-job/*"
        },
        {
            "Sid": "CreateAndReviewJobsOnConsole",
            "Effect": "Allow",
            "Action": [
                "macie2:ListClassificationJobs",
                "macie2:ListAllowLists",
                "macie2:ListCustomDataIdentifiers",
                "macie2:ListManagedDataIdentifiers",
                "macie2:SearchResources",
                "macie2:DescribeBuckets"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemple : autoriser des utilisateurs à gérer une tâche de découverte de données sensibles

Cet exemple montre comment créer une stratégie qui permet à un utilisateur d'accéder aux détails d'une tâche de découverte de données sensibles particulière, la tâche dont l'ID est `3ce05dbb7ec5505def334104bexample` L'exemple permet également à l'utilisateur de modifier le statut de la tâche si nécessaire.

La première instruction de l'exemple octroie `macie2:DescribeClassificationJob` des `macie2:UpdateClassificationJob` autorisations à l'utilisateur. Ces autorisations permettent à l'utilisateur de récupérer les détails de la tâche et de modifier son statut, respectivement. La seconde déclaration accorde des `macie2:ListClassificationJobs` autorisations à l'utilisateur, ce qui lui permet d'accéder à la tâche en utilisant la page Jobs de la console Amazon Macie.

```
{
   "Version": "2012-10-17",
   "Statement": [
 {
         "Sid": "ManageOneJob",
         "Effect": "Allow",
         "Action": [
            "macie2:DescribeClassificationJob",
            "macie2:UpdateClassificationJob"
         ],
         "Resource": "arn:aws:macie2:*:*:classification-
job/3ce05dbb7ec5505def334104bexample"
 },
 {
         "Sid": "ListJobsOnConsole",
         "Effect": "Allow",
         "Action": "macie2:ListClassificationJobs",
         "Resource": "*"
 }
   ]
}
```

Vous pouvez également autoriser l'utilisateur à accéder aux données de journalisation (événements du journal) que Macie publie sur Amazon CloudWatch Logs pour la tâche. Pour ce faire, vous pouvez ajouter des instructions qui autorisent l'exécution d'actions CloudWatch Logs (`logs`) sur le groupe de journaux et le flux correspondant à la tâche. Par exemple :

```
"Statement": [
    {
        "Sid": "AccessLogGroupForMacieJobs",
        "Effect": "Allow",
        "Action": [
            "logs:DescribeLogGroups",
            "logs:DescribeLogStreams"
        ],
        "Resource": "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs"
    },
    {
        "Sid": "AccessLogEventsForOneMacieJob",
        "Effect": "Allow",
        "Action": "logs:GetLogEvents",
        "Resource": [
            "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs/*",
            "arn:aws:logs:*:*:log-group:aws/macie/classificationjobs:log-
stream:3ce05dbb7ec5505def334104bexample"
        ]
    }
]
```

Pour plus d'informations sur la gestion de l'accès aux CloudWatch journaux, consultez la section Présentation de la gestion des autorisations d'accès à vos ressources de CloudWatch journaux dans le guide de l'utilisateur d'Amazon CloudWatch Logs.

Exemple : autoriser des utilisateurs à examiner des résultats

Cet exemple montre comment créer une stratégie qui autorise un utilisateur à accéder aux données de résultats de recherche.

Dans cet exemple, les `macie2:GetFindingStatistics` autorisations `macie2:GetFindings` et permettent à l'utilisateur de récupérer les données à l'aide de l'API Amazon Macie ou de la console Amazon Macie. Les `macie2:ListFindings` autorisations permettent à l'utilisateur de récupérer et de consulter les données à l'aide du tableau de bord récapitulatif et des pages de résultats de la console Amazon Macie.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindings",
                "macie2:GetFindingStatistics",
                "macie2:ListFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

Vous pouvez également autoriser l'utilisateur à créer et à gérer des règles de filtrage et des règles de suppression pour les résultats. Pour ce faire, vous pouvez inclure une instruction qui accorde les autorisations suivantes : `macie2:CreateFindingsFiltermacie2:GetFindingsFilter`,`macie2:UpdateFindingsFilter`, et`macie2:DeleteFindingsFilter`. Pour permettre à l'utilisateur de gérer les règles à l'aide de la console Amazon Macie, incluez également `macie2:ListFindingsFilters` des autorisations dans la politique. Par exemple :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindings",
                "macie2:GetFindingStatistics",
                "macie2:ListFindings"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ManageRules",
            "Effect": "Allow",
            "Action": [
                "macie2:GetFindingsFilter",
                "macie2:UpdateFindingsFilter",
                "macie2:CreateFindingsFilter",
                "macie2:DeleteFindingsFilter"
            ],
```

```
            "Resource": "arn:aws:macie2:*:*:findings-filter/*"
        },
        {
            "Sid": "ListRulesOnConsole",
            "Effect": "Allow",
            "Action": "macie2:ListFindingsFilters",
            "Resource": "*"
        }
    ]
}
```

Exemple : Autoriser les utilisateurs à consulter des identifiants de données personnalisés en fonction de balises

Dans les stratégies basées sur l'identité, vous pouvez utiliser des conditions pour contrôler l'accès aux ressources Amazon Macie Cet exemple montre comment créer une politique qui permet à un utilisateur d'afficher des identifiants de données personnalisés à l'aide de la console Amazon Macie Toutefois, l'autorisation n'est accordée que si la valeur de la `Owner` balise est le nom d'utilisateur de l'utilisateur

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewCustomDataIdentifiersIfOwner",
            "Effect": "Allow",
            "Action": "macie2:GetCustomDataIdentifier",
            "Resource": "arn:aws:macie2:*:*:custom-data-identifier/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        },
        {
            "Sid": "ListCustomDataIdentifiersOnConsoleIfOwner",
            "Effect": "Allow",
            "Action": "macie2:ListCustomDataIdentifiers",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
```

```
}
```

Dans cet exemple, si un utilisateur possédant le nom d'utilisateur `richard-roe` tente de vérifier les détails d'un identifiant de données personnalisé, celui-ci doit être balisé `Owner=richard-roe` ou`owner=richard-roe`. Dans le cas contraire, l'utilisateur se voit refuser l'accès. La clé de balise de condition `Owner` correspond aux deux `Owner` et `owner` parce que les noms de clé de condition ne sont pas sensibles à la casse Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Rôles liés à un service pour Amazon Macie

Amazon Macie utilise un rôle AWS Identity and Access Management (IAM) lié à un service nommé. `AWSServiceRoleForAmazonMacie` Ce rôle lié à un service est un rôle IAM directement lié à Macie. Il est prédéfini par Macie et inclut toutes les autorisations dont Macie a besoin pour appeler d'autres personnes Services AWS et surveiller les AWS ressources en votre nom. Macie utilise ce rôle lié au service partout Régions AWS où Macie est disponible.

Un rôle lié à un service facilite la configuration de Macie, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Macie définit les autorisations de ce rôle lié au service, et sauf indication contraire, seule Macie peut assumer le rôle. 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.

Vous devez configurer les autorisations pour autoriser une entité IAM (telle qu'un utilisateur ou un rôle) à 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. Vous ne pouvez supprimer un rôle lié à un service qu'après avoir supprimé les ressources associées. Vos ressources sont ainsi protégées, car vous ne pouvez pas involontairement supprimer l'autorisation d'accéder aux ressources.

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, reportez-vous aux Services AWS opérationnels avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Cliquez sur Oui avec un lien pour consulter la documentation relative aux rôles liés à un service pour ce service.

Rubriques

- Autorisations de rôle liées à un service pour Amazon Macie
- Création du rôle lié à un service pour Amazon Macie

- Modification du rôle lié à un service pour Amazon Macie
- Suppression du rôle lié à un service pour Amazon Macie
- Pris en charge Régions AWS pour le rôle lié au service Amazon Macie

Autorisations de rôle liées à un service pour Amazon Macie

Amazon Macie utilise le rôle lié au service nommé. `AWSServiceRoleForAmazonMacie` Ce rôle lié au service fait confiance au `macie.amazonaws.com` service pour assumer le rôle.

La politique d'autorisation pour le rôle, qui est nommée`AmazonMacieServiceRolePolicy`, permet à Macie d'effectuer des tâches telles que les suivantes sur les ressources spécifiées :

- Utilisez les actions Amazon S3 pour récupérer des informations sur les compartiments et les objets S3.
- Utilisez les actions Amazon S3 pour récupérer des objets S3.
- Utilisez AWS Organizations des actions pour récupérer des informations sur les comptes associés.
- Utilisez CloudWatch les actions Amazon Logs pour enregistrer les événements relatifs aux tâches de découverte de données sensibles.

Le rôle est configuré selon la politique d'autorisation suivante.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListAccountAliases",
        "organizations:DescribeAccount",
        "organizations:ListAccounts",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketTagging",
```

```
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite",
        "s3:GetEncryptionConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/macie/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogStreams"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/macie/*:log-stream:*"
      ]
    }
  ]
}
```

Pour plus de détails sur les mises à jour `AmazonMacieServiceRolePolicy` de la politique, consultezAmazon Macie met à jourAWSpolitiques gérées. Pour recevoir des alertes automatiques concernant les modifications apportées à cette politique, abonnez-vous au fil RSS sur la page d'historique des documents Macie.

Vous devez configurer les autorisations pour autoriser une entité IAM (telle qu'un utilisateur ou un rôle) à 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 un service pour Amazon Macie

Il n'est pas nécessaire de créer manuellement le rôle `AWSServiceRoleForAmazonMacie` lié à un service pour Amazon Macie. Lorsque vous activez Macie pour vous Compte AWS, Macie crée automatiquement le rôle lié au service pour vous.

Si vous supprimez le rôle lié au service Macie et que vous devez le créer à nouveau, vous pouvez utiliser le même processus pour recréer le rôle dans votre compte. Lorsque vous réactivez Macie, Macie crée à nouveau le rôle lié au service pour vous.

Modification du rôle lié à un service pour Amazon Macie

Amazon Macie ne vous permet pas de modifier le rôle lié au `AWSServiceRoleForAmazonMacie` service. Une fois qu'un rôle lié à un service a été créé, vous ne pouvez pas modifier le nom du rôle car différentes entités peuvent y faire référence. 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.

Suppression du rôle lié à un service pour Amazon Macie

Si vous n'avez plus besoin d'utiliser Amazon Macie, nous vous recommandons de supprimer manuellement le rôle lié au `AWSServiceRoleForAmazonMacie` service. Lorsque vous désactivez Macie, Macie ne supprime pas le rôle pour vous.

Avant de supprimer le rôle, vous devez désactiver Macie dans chaque Région AWS endroit où vous l'avez activé. Vous devez également nettoyer manuellement les ressources du rôle. Pour supprimer le rôle, vous pouvez utiliser la console IAM, le AWS CLI, ou l' AWS API. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

> **Note**
>
> Si Macie utilise le `AWSServiceRoleForAmazonMacie` rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Dans ce cas, attendez quelques minutes, puis recommencez l'opération.

Si vous supprimez le rôle `AWSServiceRoleForAmazonMacie` lié au service et que vous devez le créer à nouveau, vous pouvez le créer à nouveau en activant Macie pour votre compte. Lorsque vous réactivez Macie, Macie crée à nouveau le rôle lié au service pour vous.

Pris en charge Régions AWS pour le rôle lié au service Amazon Macie

Amazon Macie prend en charge l'utilisation du rôle `AWSServiceRoleForAmazonMacie` lié au service partout Régions AWS où Macie est disponible. Pour obtenir la liste des régions dans lesquelles Macie est actuellement disponible, consultez la section Points de terminaison et quotas Amazon Macie dans le. Références générales AWS

AWSpolitiques gérées pour Amazon Macie

Une politique gérée par AWS est une politique autonome créée et administrée par AWS. Les politiques gérées par AWS 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.

Gardez à l'esprit que les politiques gérées par AWS peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont disponibles pour tous les clients AWS. 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 stratégies gérées par AWS. Si AWS met à jour les autorisations définies dans une politique gérée par AWS, la mise à jour affecte toutes les identités de principal (utilisateurs, groupes et rôles) auxquelles la politique est associée. AWS est plus susceptible de mettre à jour une politique gérée par AWS lorsqu'un nouveau Service AWS est lancé ou que de nouvelles opérations API deviennent accessibles pour les services existants.

Pour plus d'informations, consultez la rubrique Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Amazon Macie propose plusieursAWSpolitiques gérées : les`AmazonMacieFullAccess`politique, la`AmazonMacieReadOnlyAccess`la politique, et`AmazonMacieServiceRolePolicy`politique.

Rubriques

- AWS Politique gérée par: AmazonMacieFullAccess
- AWS Politique gérée par: AmazonMacieReadOnlyAccess
- AWS Politique gérée par: AmazonMacieServiceRolePolicy
- Amazon Macie met à jourAWSpolitiques gérées

AWS Politique gérée par: AmazonMacieFullAccess

Vous pouvez joindre le`AmazonMacieFullAccess`politique à l'égard de vos entités IAM.

Cette politique accorde des autorisations administratives complètes qui autorisent une identité IAM (principal) pour créerRôle lié à un service Amazon Macieet effectuez toutes les actions de lecture et d'écriture pour Amazon Macie. Les autorisations incluent des fonctions mutantes telles que la création, la mise à jour et la suppression. Si cette politique est associée à un principal, celui-ci peut créer, récupérer et accéder à toutes les ressources, données et paramètres Macie de son compte.

Cette politique doit être associée à un principal pour que celui-ci puisse activer Macie pour son compte. Le principal doit être autorisé à créer le rôle lié au service Macie afin d'activer Macie pour son compte.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `macie2`— Permet aux administrateurs d'effectuer toutes les actions de lecture et d'écriture pour Amazon Macie.
- `iam`— Permet aux directeurs de créer des rôles liés à un service. Le`Resource`L'élément spécifie le rôle lié à un service pour Macie. Le`Condition`l'élément utilise`iam:AWSServiceName` clé de conditionet le`StringLike` opérateur de conditionnementpour restreindre les autorisations au rôle lié à un service pour Macie.
- `pricing`— Permet aux mandants de récupérer les données de tarification de leursCompte AWSà partir deAWS Billing and Cost Management. Macie utilise ces données pour calculer et afficher les coûts estimés lorsque les directeurs créent et configurent des tâches de découverte de données sensibles.

```
{
```

```
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "macie2:*"
         ],
         "Resource": "*"
      },
      {
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/macie.amazonaws.com/
AWSServiceRoleForAmazonMacie",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName": "macie.amazonaws.com"
            }
         }
      },
      {
         "Effect": "Allow",
         "Action": "pricing:GetProducts",
         "Resource": "*"
      }
   ]
}
```

AWS Politique gérée par: AmazonMacieReadOnlyAccess

Vous pouvez joindre le`AmazonMacieReadOnlyAccess`politique à l'égard de vos entités IAM.

Cette politique accorde des autorisations en lecture seule qui autorisent une identité IAM (principal) pour effectuer toutes les actions de lecture pour Amazon Macie. Les autorisations n'incluent pas les fonctions mutantes telles que la création, la mise à jour ou la suppression. Si cette politique est associée à un principal, celui-ci peut récupérer toutes les ressources, données et paramètres Macie de son compte, mais pas y accéder.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

`macie2`— Permet aux utilisateurs principaux d'effectuer toutes les actions de lecture pour Amazon Macie.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "macie2:Describe*",
            "macie2:Get*",
            "macie2:List*",
            "macie2:BatchGetCustomDataIdentifiers",
            "macie2:SearchResources"
         ],
         "Resource": "*"
      }
   ]
}
```

AWS Politique gérée par: AmazonMacieServiceRolePolicy

Vous ne pouvez pas attacher `AmazonMacieServiceRolePolicy` à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet à Macie d'effectuer des actions en votre nom. Pour plus d'informations, veuillez consulter Rôles liés à un service pour Amazon Macie.

Amazon Macie met à jourAWSpolitiques gérées

Vérifiez les détails des mises à jour deAWSpolitiques gérées pour Amazon Macie 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 fil RSS duHistorique des documents Maciepage.

Modification	Description	Date
AmazonMacieReadOnlyAccess— Ajout d'une nouvelle politique	Macie a ajouté une nouvelle politique, la`AmazonMacieReadOnlyAccess` politique. Cette politique accorde des autorisations en lecture seule qui permettent aux administrateurs de récupérer toutes les ressources, données et paramètres Macie de leur compte.	15 juin 2023
AmazonMacieFullAccess— Mise à jour d'une politique existante	Dans le`AmazonMacieFullAccess` politique, Macie a mis à jour le nom de ressource Amazon (ARN) du rôle lié au service Macie (`aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`).	30 juin 2022
AmazonMacieServiceRolePolicy— Mise à jour d'une politique existante	Macie a supprimé des actions et des ressources pour Amazon Macie Classic du`AmazonMacieServiceRolePolicy` politique. Amazon Macie Classic n'est plus disponible et n'est plus disponible. Plus précisément, Macie a supprimé toutAWS CloudTrailactions. Macie a également supprimé toutes les actions	20 mai 2022

Modification	Description	Date
	Amazon S3 pour les ressources suivantes :`arn:aws:s3:::awsmacie-*`,`arn:aws:s3:::awsmacietrail-*` , et`arn:aws:s3:::*-awsmacietrail-*` .	
AmazonMacieFullAccess— Mise à jour d'une politique existante	Macie a ajouté unAWS Billing and Cost Management(`pricing`) action en faveur du`AmazonMacieFullAccess` politique. Cette action permet aux clients de récupérer les données de tarification de leur compte. Macie utilise ces données pour calculer et afficher les coûts estimés lorsque les directeurs créent et configurent des tâches de découverte de données sensibles. Macie a également supprimé Amazon Macie Classic (`macie`) actions du`AmazonMacieFullAccess` politique.	7 mars 2022

Modification	Description	Date
AmazonMacieService RolePolicy— Mise à jour d'une politique existante	Macie a ajouté AmazonCloudWatchEnregistre les actions dans`AmazonMacieService RolePolicy` politique. Ces actions permettent à Macie de publier les événements du journal surCloudWatchJournaux pour les tâches de découverte de données sensibles.	13 avril 2021
Macie a commencé à suivre les modifications	Macie a commencé à suivre les modifications apportées à sonAWSpolitiques gérées.	13 avril 2021

Résolution des problèmes d'identité et d'accès à Amazon Macie

Les informations suivantes peuvent vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon Macie et AWS Identity and Access Management (IAM).

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Amazon Macie
- Je souhaite autoriser des personnes extérieures Compte AWS à moi à accéder à mes ressources Amazon Macie

Je ne suis pas autorisé à effectuer une action dans Amazon Macie

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `macie2:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 macie2:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `macie2:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures Compte AWS à moi à accéder à mes ressources Amazon Macie

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 Macie prend en charge ces fonctionnalités, consultezComment fonctionne Amazon Macie avec AWS Identity and Access Management.
- 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.

Journalisation et surveillance dans Amazon Macie

Amazon Macie est intégré àAWS CloudTrail, service qui enregistre les actions effectuées dans Macie par un utilisateur, un rôle ou un autreService AWS. Cela inclut les actions depuis la console Amazon Macie et les appels programmatiques aux opérations de l'API Amazon Macie. En utilisant les informations collectées par CloudTrail, vous pouvez déterminer quelles demandes ont été adressées à Macie. Pour chaque demande, vous pouvez identifier le moment où elle a été faite, l'adresse IP à partir de laquelle elle a été faite, qui l'a faite, ainsi que des détails supplémentaires. Pour plus d'informations, veuillez consulter Journalisation des appels d'API Amazon Macie à l'aide de AWS CloudTrail.

Validation de conformité pour Amazon Macie

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 de nombreux 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.

Résilience dans Amazon Macie

L'infrastructureAWS mondiale d'repose surRégions AWS des zones de disponibilité. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. 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 plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les Régions AWS et les zones de disponibilité, consultez Infrastructure mondiale d'AWS.

Sécurité de l'infrastructure dans Amazon Macie

En tant que service géré, Amazon Macie est protégé par un système de sécurité réseau AWS mondial. Pour plus d'informations sur les services de sécurité AWS et la manière dont AWS protège l'infrastructure, consultez la section Sécurité du cloud AWS. Pour concevoir votre environnement AWS en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le Security Pillar AWS Well-Architected Framework (Pilier de sécurité de l'infrastructure Well-Architected Framework).

Vous utilisez des appels d'API AWS publiés pour accéder à Macie via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et nous 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.

Amazon Macie et points de terminaison VPC d'interface () AWS PrivateLink

Si vous utilisez Amazon Virtual Private Cloud (Amazon VPC) pour héberger vos AWS ressources, vous pouvez établir une connexion privée entre votre VPC et Amazon Macie. Amazon VPC est un outil Service AWS que vous pouvez utiliser pour lancer AWS des ressources dans un réseau virtuel que vous définissez. Avec un VPC, vous contrôlez des paramètres réseau, tels que la plage d'adresses IP, les sous-réseaux, les tables de routage et les passerelles réseau.

Pour connecter votre VPC à Macie, vous devez créer un point de terminaison VPC d'interface pour Macie. Les points de terminaison de l'interface sont alimentés par AWS PrivateLinkune technologie qui vous permet d'accéder en privé aux API Amazon Macie sans passerelle Internet, appareil NAT,

AWS Direct Connect connexion VPN ou connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec les API Amazon Macie. Le trafic entre votre VPC et Macie ne quitte pas le réseau Amazon.

Chaque point de terminaison d'interface est représenté par une ou plusieurs interfaces réseau Elastic dans vos sous-réseaux. Pour plus d'informations, consultez la section Accès et Service AWS utilisation d'un point de terminaison VPC d'interface dans le guide de l'utilisateur Amazon VPC.

Rubriques

- Considérations relatives aux points de terminaison VPC Amazon Macie
- Création d'un point de terminaison VPC d'interface pour Amazon Macie

Considérations relatives aux points de terminaison VPC Amazon Macie

Amazon Macie prend en charge les points de terminaison VPC partout Régions AWS où il est actuellement disponible, à l'exception des régions Asie-Pacifique (Osaka) et Israël (Tel Aviv). Pour obtenir la liste des régions dans lesquelles Macie est actuellement disponible, consultez la section Points de terminaison et quotas Amazon Macie dans le. Références générales AWS En outre, Macie permet d'appeler toutes ses actions d'API à partir d'un VPC.

Si vous créez un point de terminaison VPC d'interface pour Macie, envisagez de faire de même pour les autres terminaux qui Services AWS fournissent un support VPC et s'intègrent à Macie, tels qu'Amazon et. EventBridge AWS Security Hub Macie et ces services peuvent ensuite utiliser des points de terminaison VPC pour l'intégration. Par exemple, si vous créez un point de terminaison VPC pour Macie et un point de terminaison VPC pour Security Hub, Macie peut utiliser son point de terminaison VPC lorsqu'il publie ses résultats sur Security Hub et Security Hub peut utiliser son point de terminaison VPC lorsqu'il reçoit les résultats. Pour plus d'informations sur les services qui prennent en charge les points de terminaison VPC, consultez le Services AWSguide de l'utilisateur AWS PrivateLink Amazon VPC qui s'intègre.

Pour des considérations supplémentaires, consultez la section Accès et Service AWS utilisation d'un point de terminaison VPC d'interface dans le guide de l'utilisateur Amazon VPC.

Notez que les politiques de point de terminaison VPC ne sont pas prises en charge pour Macie. Par défaut, l'accès complet à Macie est autorisé via le point de terminaison. Pour plus d'informations, consultez la section Gestion des identités et des accès pour les points de terminaison VPC et les services de point de terminaison VPC dans le guide de l'utilisateur Amazon VPC.

Création d'un point de terminaison VPC d'interface pour Amazon Macie

Vous pouvez créer un point de terminaison VPC d'interface pour le service Amazon Macie à l'aide de la console Amazon VPC ou du (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez la section Créer un point de terminaison VPC dans le guide de l'utilisateur Amazon VPC.

Lorsque vous créez un point de terminaison VPC pour Macie, utilisez le nom de service suivant :

- com.amazonaws.*region*.macie2

Où est le code de région correspondant à la région applicableRégion AWS.

Si vous activez le DNS privé pour le point de terminaison, vous pouvez envoyer des demandes d'API à Macie en utilisant son nom DNS par défaut pour la région, par exemple `macie2.us-east-1.amazonaws.com` pour la région USA Est (Virginie du Nord).

Pour plus d'informations, consultez la section Accès et Service AWS utilisation d'un point de terminaison VPC d'interface dans le guide de l'utilisateur Amazon VPC.

Journalisation des appels d'API Amazon Macie à l'aide de AWS CloudTrail

Amazon Macie s'intègre AWS CloudTrail à un service qui fournit un enregistrement des actions effectuées dans Macie par un utilisateur, un rôle ou un autre. Service AWS CloudTrailcapture tous les appels d'API pour Macie sous forme d'événements. Les appels capturés incluent des appels provenant de la console Amazon Macie et des appels programmatiques vers les opérations de l'API Amazon Macie.

Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un bucket Amazon Simple Storage Service (Amazon S3), y compris les événements pour Macie. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents en utilisant l'historique des événements sur la AWS CloudTrail console. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Macie, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Rubriques

- Informations sur Amazon Macie dans AWS CloudTrail
- Comprendre les entrées du fichier journal Amazon Macie

Informations sur Amazon Macie dans AWS CloudTrail

AWS CloudTrailest activé pour vous Compte AWS lorsque vous créez le compte. Lorsqu'une activité a lieu dans Amazon Macie, cette activité est enregistrée dans un CloudTrail événement avec d'autres AWS événements dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votreCompte AWS. Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur.

Pour un enregistrement continu des événements de votre régionCompte AWS, y compris ceux de Macie, créez un parcours. Un suivi permet CloudTrail de transférer des fichiers journaux vers un compartiment Amazon Simple Storage Service (Amazon S3). Par défaut, lorsque vous créez un parcours à l'aide de la AWS CloudTrail console, le parcours s'applique à tousRégions AWS.

Le journal d'activité consigne les événements de toutes les régions dans la partition AWS et livre les fichiers journaux dans le compartiment S3 de votre choix. 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 rubriques suivantes dans le AWS CloudTrailGuide de l'utilisateur :

- Création d'un journal d'activité pour votre Compte AWS
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux provenant de plusieurs régions
- Réception de fichiers CloudTrail journaux provenant de plusieurs comptes

Toutes les actions Macie sont enregistrées CloudTrail et documentées dans le manuel Amazon Macie API Reference. Par exemple, les appels au `CreateClassificationJobDescribeBuckets`, et les `ListFindings` actions 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 les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).
- 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 dans le guide de l'AWS CloudTrailutilisateur.

Comprendre les entrées du fichier journal Amazon Macie

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon Simple Storage Service (Amazon S3) que vous spécifiez. 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. AWS CloudTrailles fichiers journaux contiennent une ou plusieurs entrées de journal pour les

événements. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Les exemples suivants présentent des entrées de CloudTrail journal illustrant les événements liés aux actions d'Amazon Macie. Pour plus de détails sur les informations que peut contenir une entrée de journal, consultez la référence aux événements du CloudTrail journal dans le Guide de AWS CloudTrail l'utilisateur.

Exemple : Répertorier les résultats

L'exemple suivant montre une entrée de CloudTrail journal illustrant un événement lié à l'ListFindingsaction Macie. Dans cet exemple, un utilisateur AWS Identity and Access Management (IAM) (`Mary_Major`) a utilisé la console Amazon Macie pour récupérer un sous-ensemble d'informations relatives aux politiques actuelles relatives à son compte.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext":{
            "attributes": {
                "creationdate": "2023-11-14T15:49:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-14T16:09:56Z",
    "eventSource": "macie2.amazonaws.com",
    "eventName": "ListFindings",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/119.0.0.0 Safari/537.36",
    "requestParameters": {
        "sortCriteria": {
            "attributeName": "updatedAt",
            "orderBy": "DESC"
        },
```

```
        "findingCriteria": {
            "criterion": {
                "archived": {
                    "eq": [
                        "false"
                    ]
                },
                "category": {
                    "eq": [
                        "POLICY"
                    ]
                }
            }
        },
        "maxResults": 25,
        "nextToken": ""
    },
    "responseElements": null,
    "requestID": "d58af6be-1115-4a41-91f8-ace03example",
    "eventID": "ad97fac5-f7cf-4ff9-9cf2-d0676example",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


Exemple : extraction d'échantillons de données sensibles pour une recherche

Cet exemple montre des entrées de CloudTrail journal illustrant les événements relatifs à la récupération et à la révélation d'échantillons de données sensibles signalés par Macie dans une constatation. Dans cet exemple, un utilisateur IAM (`JohnDoe`) a utilisé la console Amazon Macie pour récupérer et révéler des échantillons de données sensibles. Le compte Macie de l'utilisateur est configuré pour assumer un rôle IAM (`MacieReveal`) afin de récupérer et de révéler des échantillons de données sensibles.

L'événement de journal suivant indique les détails de la demande de l'utilisateur visant à récupérer et à révéler des échantillons de données sensibles en exécutant l'GetSensitiveDataOccurrencesaction Macie.


```
{
    "eventVersion": "1.08",
```

```
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "UU4MH7OYK5ZCOAEXAMPLE:JohnDoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/JohnDoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "UU4MH7OYK5ZCOAEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-12-12T14:40:23Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-12-12T17:04:47Z",
    "eventSource": "macie2.amazonaws.com",
    "eventName": "GetSensitiveDataOccurrences",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "198.51.100.252",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/119.0.0.0 Safari/537.36",
    "requestParameters": {
        "findingId": "3ad9d8cd61c5c390bede45cd2example"
    },
    "responseElements": null,
    "requestID": "c30cb760-5102-47e7-88d8-ff2e8example",
    "eventID": "baf52d92-f9c3-431a-bfe8-71c81example",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


L'événement de journal suivant indique des détails sur Macie qui assume alors le rôle IAM spécifié (`MacieReveal`) en exécutant l'action AWS Security Token Service (AWS STS) AssumeRole.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "reveal-samples.macie.amazonaws.com"
    },
    "eventTime": "2023-12-12T17:04:47Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "reveal-samples.macie.amazonaws.com",
    "userAgent": "reveal-samples.macie.amazonaws.com",
    "requestParameters": {
        "roleArn": "arn:aws:iam::111122223333:role/MacieReveal",
        "roleSessionName": "RevealCrossAccount"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
            "sessionToken": "XXYYaz...
EXAMPLE_SESSION_TOKEN
XXyYaZAz",
            "expiration": "Dec 12, 2023, 6:04:47 PM"
        },
        "assumedRoleUser": {
            "assumedRoleId": "AROAXOTKAROCSNEXAMPLE:RevealCrossAccount",
            "arn": "arn:aws:sts::111122223333:assumed-role/MacieReveal/
RevealCrossAccount"
        }
    },
    "requestID": "d905cea8-2dcb-44c1-948e-19419example",
    "eventID": "74ee4d0c-932d-3332-87aa-8bcf3example",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::IAM::Role",
            "ARN": "arn:aws:iam::111122223333:role/MacieReveal"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
```

```
    "eventCategory": "Management"
}
```

Marquage des ressources Amazon Macie

Une étiquette est une étiquette facultative que vous pouvez définir et attribuer à AWS des ressources, notamment à certains types de ressources Amazon Macie. Les balises peuvent vous aider à identifier, classer et gérer les ressources de différentes manières, par exemple en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Par exemple, vous pouvez utiliser des balises pour appliquer des politiques, répartir les coûts, distinguer les versions des ressources ou identifier les ressources qui répondent à certaines exigences de conformité ou à certains flux de travail.

Vous pouvez attribuer des balises aux types de ressources Macie suivants : listes d'autorisation, identifiants de données personnalisés, règles de filtrage et règles de suppression pour les résultats et tâches de découverte de données sensibles. Si vous êtes l'administrateur Macie d'une organisation, vous pouvez également attribuer des balises aux comptes des membres de votre organisation.

Rubriques

Principes fondamentaux du balisage

Une ressource peut avoir jusqu'à 50 balises. Chaque balise est constituée d'une clé de balise obligatoire et d'une valeur de balise facultative que vous définissez. Une clé de balise est une étiquette générale qui fait office de catégorie pour une valeur de balise plus spécifique. Une valeur de balise tient lieu de descripteur pour une clé de balise.

Par exemple, si vous créez des identifiants de données personnalisés et des tâches de découverte de données sensibles pour analyser des données à différents moments d'un flux de travail (un ensemble pour les données intermédiaires et un autre pour les données de production), vous pouvez attribuer une clé de `Stack` balise à ces ressources. La valeur de balise de cette clé de balise peut

`Staging` concerner des identificateurs de données personnalisés et des tâches conçues pour analyser des données intermédiaires, ainsi que `Production` pour les autres.

Lorsque vous définissez et attribuez des balises aux ressources, gardez à l'esprit les points suivants :

- Chaque ressource peut avoir un maximum de 50 balises.
- Pour chaque ressource, chaque clé de balise doit être unique et ne peut comporter qu'une seule valeur de balise.
- Les clés et valeurs de balise sont sensibles à la casse. Nous vous recommandons de définir une stratégie de mise en majuscule des balises et de mettre en œuvre cette stratégie de manière cohérente dans l'ensemble de vos ressources.
- Une clé de balise peut comporter au maximum 128 caractères UTF-8. La valeur d'une balise peut comporter au maximum 256 caractères UTF-8. Les caractères peuvent être des lettres, des chiffres, des espaces ou les symboles suivants : _. :/= + - @
- Le `aws:` préfixe est réservé à l'usage deAWS. Vous ne pouvez pas l'utiliser dans les clés ou les valeurs de balise que vous définissez. En outre, vous ne pouvez ni modifier ni supprimer les clés ou les valeurs de balise qui utilisent ce préfixe. Les balises qui utilisent ce préfixe ne sont pas comptabilisées dans le quota de 50 balises par ressource.
- Toutes les balises que vous attribuez ne sont disponibles que pour vous Compte AWS et uniquement dans la zone Région AWS dans laquelle vous les attribuez.
- Si vous supprimez une ressource, toutes les balises qui lui sont attribuées sont également supprimées.

Pour obtenir des restrictions supplémentaires, des conseils et des bonnes pratiques, consultez le Guide de l'utilisateur AWS des ressources de balisage.

> **Important**
>
> Ne stockez pas de données confidentielles ou d'autres types de données sensibles dans des balises. Les tags sont accessibles depuis de nombreux Services AWS sites, notammentAWS Billing and Cost Management. Ils ne sont pas destinés à être utilisés pour des données sensibles.

Pour ajouter et gérer des balises pour les ressources Macie, vous pouvez utiliser la console Amazon Macie, l'API Amazon Macie, l'éditeur de balises de la AWS Resource Groups console ou l'AWS

Resource GroupsAPI de balisage. Avec Macie, vous pouvez ajouter des balises à une ressource lorsque vous la créez. Vous pouvez également ajouter et gérer des balises pour des ressources existantes individuelles. Les groupes de ressources vous permettent d'ajouter et de gérer des balises de manière groupée pour plusieurs ressources existantesServices AWS, y compris Macie. Pour plus d'informations, consultez le Guide de l'utilisateur de la balisage des ressources AWS.

Utilisation de balises dans les politiques IAM

Après avoir commencé à baliser les ressources, vous pouvez définir des autorisations au niveau des ressources basées sur des balises dans les politiques AWS Identity and Access Management (IAM). En utilisant les balises de cette manière, vous pouvez mettre en œuvre un contrôle précis des utilisateurs et des rôles autorisés à créer et à baliser des ressources, et des utilisateurs et des rôles autorisés à ajouter, modifier et supprimer des balises de manière plus générale. Compte AWS Pour contrôler l'accès en fonction des balises, vous pouvez utiliser des clés de condition liées aux balises dans l'élément Condition des politiques IAM.

Par exemple, vous pouvez créer une politique qui permet à un utilisateur d'avoir un accès complet à toutes les ressources Amazon Macie, si la `Owner` balise de la ressource indique son nom d'utilisateur :

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "macie2:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

Si vous définissez des autorisations au niveau des ressources basées sur des balises, les autorisations prennent effet immédiatement. Vos ressources sont ainsi plus sécurisées dès leur création et vous pouvez rapidement commencer à appliquer l'utilisation des balises pour les nouvelles ressources. Vous pouvez également utiliser des autorisations au niveau des ressources

afin de contrôler les clés et les valeurs de balise qui peuvent être associés à des ressources nouvelles et existantes. Pour plus d'informations, consultez la section Contrôle de l'accès aux ressources AWS à l'aide de balises du Guide de l'utilisateur IAM.

Ajouter des balises aux ressources Amazon Macie

Pour ajouter des balises à une ressource Amazon Macie individuelle, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie. Pour ajouter des balises à plusieurs ressources Macie en même temps, utilisez l'éditeur de balises de la AWS Resource Groups console ou les opérations de balisage de l'API de AWS Resource Groupsbalisage.

> **Important**
>
> L'ajout de balises à une ressource peut affecter l'accès à la ressource. Avant d'ajouter une balise à une ressource, passez en revue les politiques AWS Identity and Access Management (IAM) susceptibles d'utiliser des balises pour contrôler l'accès aux ressources.

Console

Lorsque vous créez une liste d'autorisation, un identifiant de données personnalisé ou une tâche de découverte de données sensibles, la console Amazon Macie propose des options permettant d'ajouter des balises à la ressource. Suivez les instructions de la console pour ajouter des balises à ces types de ressources lors de leur création. Pour ajouter des balises à une règle de filtre ou de suppression ou à un compte de membre dans une organisation, vous devez créer la ressource avant de pouvoir y ajouter des balises.

Pour ajouter une ou plusieurs balises à une ressource existante à l'aide de la console Amazon Macie, procédez comme suit.

Pour ajouter une étiquette à une ressource

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Selon le type de ressource auquel vous souhaitez ajouter une balise, effectuez l'une des opérations suivantes :

   - Pour obtenir une liste d'autorisations, choisissez Listes d'autorisation dans le volet de navigation.

Ensuite, dans le tableau, cochez la case correspondant à la liste. Choisissez ensuite Gérer les balises dans le menu Actions.

- Pour un identifiant de données personnalisé, choisissez Identifiants de données personnalisés dans le volet de navigation.

  Ensuite, dans le tableau, cochez la case correspondant à l'identifiant de données personnalisé. Choisissez ensuite Gérer les balises dans le menu Actions.

- Pour un filtre ou une règle de suppression, choisissez Résultats dans le volet de navigation.

  Ensuite, dans la liste des règles enregistrées, choisissez l'icône d'édition () à côté de la règle. Ensuite, sélectionnez Gérer les balises.

- Pour un compte de membre au sein de votre organisation, choisissez Comptes dans le volet de navigation.

  Ensuite, dans le tableau, cochez la case correspondant au compte. Choisissez ensuite Gérer les balises dans le menu Actions.

- Pour une tâche de découverte de données sensibles, choisissez Jobs dans le volet de navigation.

  Ensuite, dans le tableau, cochez la case correspondant à la tâche. Choisissez ensuite Gérer les balises dans le menu Actions.

La fenêtre Gérer les balises répertorie toutes les balises actuellement attribuées à la ressource.

3. Dans la fenêtre Gérer les balises, choisissez Modifier les balises.
4. Choisissez Ajouter une balise.
5. Dans la zone Clé, entrez la clé de balise pour la balise à ajouter à la ressource. Ensuite, dans la zone Valeur, entrez éventuellement une valeur de balise pour la clé.

   Une clé de balise peut contenir jusqu'à 128 caractères. Une valeur de balise peut contenir jusqu'à 256 caractères. Les caractères peuvent être des lettres, des chiffres, des espaces ou les symboles suivants : _. :/= + - @

6. (Facultatif) Pour ajouter une autre balise à la ressource, choisissez Ajouter une étiquette, puis répétez l'étape précédente. Vous pouvez attribuer jusqu'à 50 balises à une ressource.
7. Lorsque vous avez fini d'ajouter des balises, choisissez Enregistrer.

API

Pour créer une ressource et y ajouter une ou plusieurs balises par programmation, utilisez l'`Create`opération appropriée au type de ressource que vous souhaitez créer :

- Liste d'autorisations : utilisez l'CreateAllowListopération ou, si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la create-allow-listcommande.
- Identifiant de données personnalisé : utilisez l'CreateCustomDataIdentifieropération ou, si vous utilisez leAWS CLI, exécutez la create-custom-data-identifiercommande.
- Règle de filtrage ou de suppression : utilisez l'CreateFindingsFilteropération ou, si vous utilisez laAWS CLI, exécutez la create-findings-filtercommande.
- Compte membre : utilisez l'CreateMemberopération ou, si vous utilisez laAWS CLI, exécutez la commande create-member.
- Tâche de découverte de données sensibles : utilisez l'CreateClassificationJobopération ou, si vous utilisez laAWS CLI, exécutez la create-classification-jobcommande.

Dans votre demande, utilisez le `tags` paramètre pour spécifier la clé de balise (`key`) et la valeur de balise facultative (`value`) pour chaque balise à ajouter à la ressource. Le `tags` paramètre spécifie une string-to-string carte des clés de balise et de leurs valeurs de balise associées.

Pour ajouter une ou plusieurs balises à une ressource existante, utilisez le TagResourcefonctionnement de l'API Amazon Macie ou, si vous utilisez laAWS CLI, exécutez la commande tag-resource. Dans votre demande, spécifiez l'Amazon Resource Name (ARN) de la ressource à laquelle vous souhaitez ajouter un tag. Utilisez le `tags` paramètre pour spécifier la clé de balise (`key`) et la valeur de balise facultative (`value`) pour chaque balise à ajouter à la ressource. Comme c'est le cas pour les `Create` opérations et les commandes, le `tags` paramètre spécifie une string-to-string carte des clés de balise et de leurs valeurs de balise associées.

Par exemple, la AWS CLI commande suivante ajoute une clé de `Stack` balise avec une valeur de `Production` balise à la tâche spécifiée. Cet exemple est formaté pour Microsoft Windows et utilise le caractère de continuation de ligne caret (^) pour améliorer la lisibilité.

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Production\"}
```

Où :

- `resource-arn`spécifie l'ARN de la tâche à laquelle ajouter une balise.
- *`Stack`*est la clé de balise de la balise à ajouter à la tâche.
- *`Production`*est la valeur de balise pour la clé de balise spécifiée (*`Stack`*).

Dans l'exemple suivant, la commande ajoute plusieurs balises à la tâche :

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Production\",\"CostCenter\":\"12345\",\"Owner\":\"jane-doe\"}
```

Pour chaque balise d'une `tags` carte, les `value` arguments `key` et sont obligatoires. Toutefois, la valeur de l'`value`argument peut être une chaîne vide. Si vous ne souhaitez pas associer une valeur de balise à une clé de balise, ne spécifiez pas de valeur pour l'`value`argument. Par exemple, la AWS CLI commande suivante ajoute une clé de `Owner` balise sans valeur de balise associée :

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Owner\":\"\"}
```

Si une opération de balisage aboutit, Macie renvoie une réponse HTTP 204 vide. Dans le cas contraire, Macie renvoie une réponse HTTP 4 xx ou 500 indiquant pourquoi l'opération a échoué.

Révision des balises pour les ressources Amazon Macie

Vous pouvez consulter les balises (clés et valeurs de balise) d'une ressource Amazon Macie à l'aide de la console Amazon Macie ou de l'API Amazon Macie. Si vous préférez le faire pour plusieurs

ressources Macie en même temps, vous pouvez utiliser l'éditeur de balises sur la AWS Resource Groups console ou les opérations de balisage de l'API de AWS Resource Groupsbalisage.

Console

Suivez ces étapes pour vérifier les balises d'une ressource à l'aide de la console Amazon Macie.

Pour consulter les balises d'une ressource

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Selon le type de ressource dont vous souhaitez consulter les balises, effectuez l'une des opérations suivantes :

   - Pour obtenir une liste d'autorisations, choisissez Listes d'autorisation dans le volet de navigation.

     Ensuite, dans le tableau, cochez la case correspondant à la liste. Choisissez ensuite Gérer les balises dans le menu Actions.
   - Pour un identifiant de données personnalisé, choisissez Identifiants de données personnalisés dans le volet de navigation.

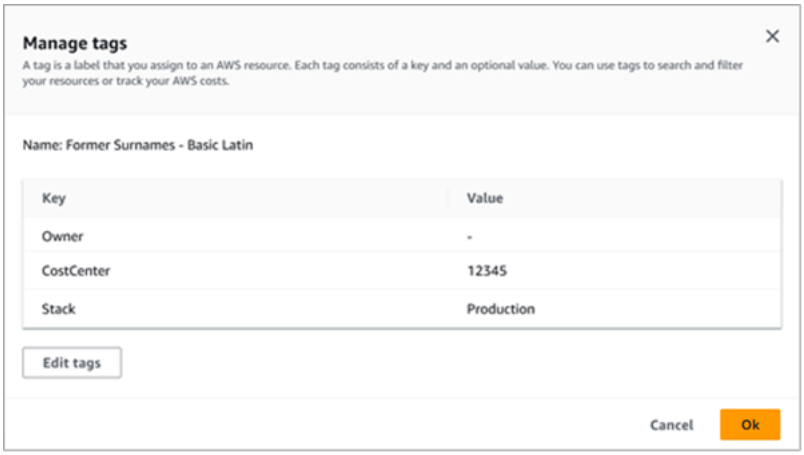
     Ensuite, dans le tableau, cochez la case correspondant à l'identifiant de données personnalisé. Choisissez ensuite Gérer les balises dans le menu Actions.
   - Pour un filtre ou une règle de suppression, choisissez Résultats dans le volet de navigation.

     Ensuite, dans la liste des règles enregistrées, choisissez l'icône d'édition (✎) à côté de la règle. Ensuite, sélectionnez Gérer les balises.
   - Pour un compte de membre au sein de votre organisation, choisissez Comptes dans le volet de navigation.

     Ensuite, dans le tableau, cochez la case correspondant au compte. Choisissez ensuite Gérer les balises dans le menu Actions.
   - Pour une tâche de découverte de données sensibles, choisissez Jobs dans le volet de navigation.

     Ensuite, dans le tableau, cochez la case correspondant à la tâche. Choisissez ensuite Gérer les balises dans le menu Actions.

La fenêtre Gérer les balises répertorie toutes les balises actuellement attribuées à la ressource. Par exemple, l'image suivante montre les balises attribuées à un identifiant de données personnalisé.



Dans cet exemple, trois balises sont attribuées à l'identifiant de données personnalisé : la clé de balise Owner sans valeur de CostCenterbalise associée ; la clé de balise associée à 12345 ; et la clé de balise Stack avec Production comme valeur de balise associée.

3. Lorsque vous avez terminé de vérifier les balises, choisissez Annuler pour fermer la fenêtre.

API

Pour récupérer et vérifier les balises d'une ressource existante par programmation, vous pouvez utiliser l'`Describe`opération `Get` or appropriée au type de ressource pour lequel vous souhaitez consulter les balises. Par exemple, si vous utilisez l'GetCustomDataIdentifieropération ou si vous exécutez la get-custom-data-identifiercommande à partir du AWS Command Line Interface (AWS CLI), la réponse inclut un `tags` objet. L'objet répertorie toutes les balises (clés et valeurs de balise) actuellement attribuées à la ressource.

Vous pouvez également utiliser le ListTagsForResourcefonctionnement de l'API Amazon Macie. Dans votre demande, utilisez le `resourceArn` paramètre pour spécifier le nom de ressource Amazon (ARN) de la ressource. Si vous utilisez leAWS CLI, exécutez la list-tags-for-resourcecommande et utilisez le `resource-arn` paramètre pour spécifier l'ARN de la ressource. Par exemple :

```
C:\> aws macie2 list-tags-for-resource --resource-arn arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample
```

Dans l'exemple précédent, *arn:aws:macie2:us-east-1:123456789012:classification-job/3ce05dbb7ec5505def334104bexample* est l'ARN d'une tâche de découverte de données sensibles existante.

Si l'opération aboutit, Macie renvoie un `tags` objet qui répertorie toutes les balises (clés et valeurs de balise) actuellement attribuées à la ressource. Par exemple :

```
{
    "tags": {
        "Stack": "Production",
        "CostCenter": "12345",
        "Owner": ""
    }
}
```

Où `Stack``CostCenter`, et `Owner` sont les clés de balise attribuées à la ressource. `Production`est la valeur de balise associée à la clé de `Stack` balise. `12345`est la valeur de balise associée à la clé de `CostCenter` balise. Aucune valeur de `Owner` balise n'est associée à la clé de balise.

Pour récupérer la liste de toutes les ressources Macie dotées de balises et de toutes les balises attribuées à chacune de ces ressources, utilisez le GetResourcesfonctionnement de l'API de AWS Resource Groups balisage. Dans votre demande, définissez la valeur du `ResourceTypeFilters` paramètre sur`macie2`. Pour ce faireAWS CLI, exécutez la commande get-resources et définissez la valeur du `resource-type-filters` paramètre sur. `macie2` Par exemple :

```
C:\> aws resourcegroupstaggingapi get-resources --resource-type-filters "macie2"
```

Si l'opération aboutit, Resource Groups renvoie un `ResourceTagMappingList` tableau contenant les ARN de toutes les ressources Macie dotées de balises, ainsi que les clés et les valeurs de balise attribuées à chacune de ces ressources.

Modification des balises pour les ressources Amazon Macie

Pour modifier les balises (clés ou valeurs de balises) d'une ressource Amazon Macie, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie. Pour ce faire pour plusieurs ressources Macie en même temps, utilisez l'éditeur de balises de la AWS Resource Groups console ou les opérations de balisage de l'API de AWS Resource Groupsbalisage.

> **Important**
>
> La modification des balises d'une ressource peut affecter l'accès à la ressource. Avant de modifier la clé ou la valeur d'une balise pour une ressource, passez en revue les politiques AWS Identity and Access Management (IAM) susceptibles d'utiliser la balise pour contrôler l'accès aux ressources.

Console

Suivez ces étapes pour modifier les balises d'une ressource à l'aide de la console Amazon Macie.

Pour modifier les balises d'une ressource

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Selon le type de ressource dont vous souhaitez modifier les balises, effectuez l'une des opérations suivantes :
   - Pour obtenir une liste d'autorisations, choisissez Listes d'autorisation dans le volet de navigation.

     Ensuite, dans le tableau, cochez la case correspondant à la liste. Choisissez ensuite Gérer les balises dans le menu Actions.
   - Pour un identifiant de données personnalisé, choisissez Identifiants de données personnalisés dans le volet de navigation.

     Ensuite, dans le tableau, cochez la case correspondant à l'identifiant de données personnalisé. Choisissez ensuite Gérer les balises dans le menu Actions.
   - Pour un filtre ou une règle de suppression, choisissez Résultats dans le volet de navigation.

     Ensuite, dans la liste des règles enregistrées, choisissez l'icône d'édition () à côté de la règle. Ensuite, sélectionnez Gérer les balises.
   - Pour un compte de membre au sein de votre organisation, choisissez Comptes dans le volet de navigation.

Ensuite, dans le tableau, cochez la case correspondant au compte. Choisissez ensuite Gérer les balises dans le menu Actions.

- Pour une tâche de découverte de données sensibles, choisissez Jobs dans le volet de navigation.

  Ensuite, dans le tableau, cochez la case correspondant à la tâche. Choisissez ensuite Gérer les balises dans le menu Actions.

La fenêtre Gérer les balises répertorie toutes les balises actuellement attribuées à la ressource.

3. Dans la fenêtre Gérer les balises, choisissez Modifier les balises.
4. Effectuez l'une des actions suivantes :

   - Pour ajouter une valeur de balise à une clé de balise, entrez la valeur dans la zone Valeur à côté de la clé de balise.
   - Pour modifier une clé de balise existante, choisissez Supprimer à côté de la balise. Choisissez ensuite Ajouter un tag. Dans la zone Clé qui apparaît, entrez la nouvelle clé de tag. Entrez éventuellement une valeur de balise associée dans la zone Valeur.
   - Pour modifier une valeur de balise existante, choisissez X dans la zone Valeur qui contient la valeur. Entrez ensuite la nouvelle valeur de balise dans la zone Valeur.
   - Pour supprimer une valeur de balise existante, choisissez X dans la zone Valeur qui contient la valeur.
   - Pour supprimer une balise existante (à la fois la clé et la valeur de la balise), choisissez Supprimer à côté de la balise.

   Une ressource peut avoir jusqu'à 50 balises. Une clé de balise peut contenir jusqu'à 128 caractères. Une valeur de balise peut contenir jusqu'à 256 caractères. Les caractères peuvent être des lettres, des chiffres, des espaces ou les symboles suivants : _. :/= + - @
5. Lorsque vous avez fini de modifier les balises, choisissez Enregistrer.

API

Lorsque vous modifiez une balise pour une ressource par programmation, vous remplacez la balise existante par de nouvelles valeurs. Par conséquent, la meilleure façon de modifier une

balise varie selon que vous souhaitez modifier une clé de balise, une valeur de balise ou les deux. Pour modifier une clé de balise, supprimez la balise actuelle et ajoutez-en une nouvelle.

Pour modifier ou supprimer uniquement la valeur de balise associée à une clé de balise, remplacez la valeur existante en utilisant le TagResourcefonctionnement de l'API Amazon Macie ou, si vous utilisez le AWS Command Line Interface (AWS CLI), en exécutant la commande tag-resource. Dans votre demande, spécifiez le nom de ressource Amazon (ARN) de la ressource dont vous souhaitez modifier ou supprimer la valeur de balise.

Pour modifier la valeur de balise d'une clé de balise, utilisez le `tags` paramètre pour spécifier la clé de balise dont vous souhaitez modifier la valeur de balise, puis spécifiez la nouvelle valeur de balise pour la clé. Par exemple, la commande suivante modifie la valeur de balise de `Production` à `Staging` pour la clé de `Stack` balise affectée à la tâche de découverte de données sensibles spécifiée. Cet exemple est formaté pour Microsoft Windows et utilise le caractère de continuation de ligne caret (^) pour améliorer la lisibilité.

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"Staging\"}
```

Où :

- `resource-arn`spécifie l'ARN de la tâche.
- *`Stack`*est la clé de balise associée à la valeur de balise à modifier.
- *`Staging`*est la nouvelle valeur de balise pour la clé de balise spécifiée (*`Stack`*).

Pour supprimer une valeur de balise d'une clé de balise, ne spécifiez pas de valeur pour l'`value`argument dans le `tags` paramètre. Par exemple :

```
C:\> aws macie2 tag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tags={\"Stack\":\"\"}
```

Si l'opération aboutit, Macie renvoie une réponse HTTP 204 vide. Dans le cas contraire, Macie renvoie une réponse HTTP 4 xx ou 500 indiquant pourquoi l'opération a échoué.

Supprimer des balises des ressources Amazon Macie

Pour supprimer des balises d'une ressource Amazon Macie, vous pouvez utiliser la console Amazon Macie ou l'API Amazon Macie. Pour ce faire pour plusieurs ressources Macie en même temps, utilisez l'éditeur de balises de la AWS Resource Groups console ou les opérations de balisage de l'API de AWS Resource Groupsbalisage.

> **Important**
>
> La suppression des balises d'une ressource peut affecter l'accès à la ressource. Avant de supprimer une balise, passez en revue les politiques AWS Identity and Access Management (IAM) susceptibles d'utiliser la balise pour contrôler l'accès aux ressources.

Console

Suivez ces étapes pour supprimer une ou plusieurs balises d'une ressource à l'aide de la console Amazon Macie.

Pour supprimer un tag d'une ressource

1. Ouvrez la console Amazon Macie à l'adresse https://console.aws.amazon.com/macie/.
2. Selon le type de ressource dont vous souhaitez supprimer une balise, effectuez l'une des opérations suivantes :

   - Pour obtenir une liste d'autorisations, choisissez Listes d'autorisation dans le volet de navigation.

     Ensuite, dans le tableau, cochez la case correspondant à la liste. Choisissez ensuite Gérer les balises dans le menu Actions.
   - Pour un identifiant de données personnalisé, choisissez Identifiants de données personnalisés dans le volet de navigation.

     Ensuite, dans le tableau, cochez la case correspondant à l'identifiant de données personnalisé. Choisissez ensuite Gérer les balises dans le menu Actions.
   - Pour un filtre ou une règle de suppression, choisissez Résultats dans le volet de navigation.

Ensuite, dans la liste des règles enregistrées, choisissez l'icône d'édition () à côté de la règle. Ensuite, sélectionnez Gérer les balises.

- Pour un compte de membre au sein de votre organisation, choisissez Comptes dans le volet de navigation.

  Ensuite, dans le tableau, cochez la case correspondant au compte. Choisissez ensuite Gérer les balises dans le menu Actions.

- Pour une tâche de découverte de données sensibles, choisissez Jobs dans le volet de navigation.

  Ensuite, dans le tableau, cochez la case correspondant à la tâche. Choisissez ensuite Gérer les balises dans le menu Actions.

La fenêtre Gérer les balises répertorie toutes les balises actuellement attribuées à la ressource.

3. Dans la fenêtre Gérer les balises, choisissez Modifier les balises.
4. Effectuez l'une des actions suivantes :

   - Pour supprimer uniquement la valeur d'une balise, choisissez X dans la zone Valeur qui contient la valeur à supprimer.
   - Pour supprimer à la fois la clé de balise et la valeur de balise (par paire) d'une balise, choisissez Supprimer à côté de la balise à supprimer.
5. (Facultatif) Pour supprimer d'autres balises de la ressource, répétez l'étape précédente pour chaque balise supplémentaire à supprimer.
6. Lorsque vous avez terminé de supprimer les balises, choisissez Enregistrer.

API

Pour supprimer une ou plusieurs balises d'une ressource par programmation, utilisez le UntagResourcefonctionnement de l'API Amazon Macie. Dans votre demande, utilisez le `resourceArn` paramètre pour spécifier le nom de ressource Amazon (ARN) de la ressource dont vous souhaitez supprimer une balise. Utilisez le `tagKeys` paramètre pour spécifier la clé de la balise à supprimer. Pour supprimer uniquement une valeur de balise spécifique (et non une clé de balise) d'une ressource, modifiez la balise au lieu de la supprimer.

Si vous utilisez le AWS Command Line Interface (AWS CLI), exécutez la commande untag-resource et utilisez le `resource-arn` paramètre pour spécifier l'ARN de la ressource dont vous souhaitez supprimer une balise. Utilisez le `tag-keys` paramètre pour spécifier la clé de la balise à supprimer. Par exemple, la commande suivante supprime la `Stack` balise (à la fois la clé et la valeur de balise) de la tâche de découverte de données sensibles spécifiée :

```
C:\> aws macie2 untag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tag-keys Stack
```

Où `resource-arn` spécifie l'ARN de la tâche dont vous souhaitez supprimer une balise, et *`Stack`* est la clé de balise de la balise à supprimer.

Pour supprimer plusieurs balises d'une ressource, ajoutez chaque clé de balise supplémentaire comme argument pour le `tag-keys` paramètre. Par exemple :

```
C:\> aws macie2 untag-resource ^
--resource-arn arn:aws:macie2:us-east-1:123456789012:classification-
job/3ce05dbb7ec5505def334104bexample ^
--tag-keys Stack Owner
```

Où `resource-arn` indique l'ARN de la tâche dont vous souhaitez supprimer les balises, *`Stack`* et où *`Owner`* sont les clés de balise des balises à supprimer.

Si l'opération aboutit, Macie renvoie une réponse HTTP 204 vide. Dans le cas contraire, Macie renvoie une réponse HTTP 4 xx ou 500 indiquant pourquoi l'opération a échoué.

Création de ressources Amazon Macie avec AWS CloudFormation

Amazon Macie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie ie et de votre infrastructure. AWS CloudFormation AWS Vous créez un modèle qui décrit toutes les AWS ressources que vous souhaitez utiliser, et AWS CloudFormation alloue et configure ces ressources.

Lorsque vous utilisezAWS CloudFormation, vous pouvez réutiliser votre modèle pour configurer vos ressources Décrivez vos ressources une seule fois, puis allouez-les de façon répétée dans plusieurs comptes Comptes AWS etRégions AWS.

Rubriques

- Amazon Macie ie ie ie ie ie ie ie AWS CloudFormation
- En savoir plus sur AWS CloudFormation

Amazon Macie ie ie ie ie ie ie ie AWS CloudFormation

Pour allouer et configurer des ressources pour Amazon Macie ie ie ie et les services associés, vous devez maîtriser les AWS CloudFormationmodèles. Les modèles sont des fichiers texte au format JSON ou YAML. Ces modèles décrivent les ressources que vous souhaitez allouer dans vos piles AWS CloudFormation.

Si le format JSON ou YAML ne vous est pas familier, vous pouvez utiliser AWS CloudFormation Designer, un outil graphique destiné à la création et la modification AWS CloudFormation de modèles. Avec Designer, vous pouvez créer un diagramme des ressources de votre modèle à l'aide d'une drag-and-drop interface, puis en modifier les détails à l'aide de l'un éditeur JSON et YAML intégré. Pour plus d'informations, consultez Qu'est-ce que AWS CloudFormation Designer ? dans le AWS CloudFormationGuide de l'utilisateur.

Vous pouvez créer des AWS CloudFormation modèles pour les types de ressources Macie suivants :

- Autoriser les listes
- Identificateurs des données personnalisés
- Règles de filtrage et règles de suppression pour les résultats, également appelées filtres de résultats

Pour de plus amples informations, y compris des exemples de modèles JSON et YAML pour ces types de ressources, consultez la Référence de type de ressource Amazon Macie ie ie ie ie ie ie ie AWS CloudFormation

En savoir plus sur AWS CloudFormation

Pour en savoir plus surAWS CloudFormation, consultez les ressources suivantes :

- AWS CloudFormation
- Guide de l'utilisateur AWS CloudFormation
- Référence API AWS CloudFormation
- Guide de l'utilisateur de l'interface de ligne de commande AWS CloudFormation

Suspension ou désactivation d'Amazon Macie

Vous pouvez suspendre ou désactiver Amazon Macie dans unRégion AWSen utilisant la console Amazon Macie ou l'API Amazon Macie. Macie cesse alors d'effectuer toutes les activités liées à votre compte dans cette région. Vous n'êtes pas facturé pour l'utilisation de Macie dans la région lorsque celle-ci est suspendue ou désactivée.

Si vous suspendez ou désactivez Macie, vous pourrez la réactiver ultérieurement.

Rubriques

Suspension d'Amazon Macie

Si vous suspendez Amazon Macie, Macie conserve l'identifiant de session, les paramètres et les ressources de votre compte dans leRégion AWS. Par exemple, vos résultats existants restent intacts et sont conservés jusqu'à 90 jours. Toutefois, lorsque vous suspendez Macie, elle cesse d'effectuer toutes les activités liées à votre compte dans la région concernée. Cela inclut la surveillance de vos données Amazon Simple Storage Service (Amazon S3), la découverte automatique de données sensibles et l'exécution de toutes les tâches de découverte de données sensibles actuellement en cours. Macie annule également toutes vos tâches de découverte de données sensibles dans la Région.

Après avoir suspendu Macie, vous pouvez le réactiver. Vous retrouvez ensuite l'accès à vos paramètres et à vos ressources dans la région concernée, et Macie reprend ses activités pour votre compte dans cette région. Cela inclut la mise à jour de l'inventaire du compartiment S3 pour votre compte et la surveillance de ces compartiments pour la sécurité et le contrôle de l'accès. Cela n'inclut pas la reprise ou le redémarrage de vos tâches de découverte de données sensibles. Les tâches de découverte de données sensibles ne peuvent pas être reprises ni redémarrées après leur annulation.

Cette rubrique explique comment suspendre Macie à l'aide de la console Amazon Macie. Si vous préférez le faire par programmation, vous pouvez utiliserUpdateMacieSessionfonctionnement de l'API Amazon Macie.

> **Note**
>
> Si vous êtes l'administrateur Macie d'une organisation, vous devez supprimer tous les comptes membres associés à votre compte avant de suspendre Macie pour votre compte. Pour plus d'informations, veuillez consulter Gestion de plusieurs comptes .

Pour suspendre Macie

1. Ouvrez la console Amazon Macie à l'adressehttps://console.aws.amazon.com/macie/.
2. En utilisant leRégion AWSdans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez suspendre Macie.
3. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
4. ChoisissezSuspendre Macie.
5. Lorsque vous êtes invité à confirmer, entrez**`Suspend`**, puis choisissezSuspendre.

Pour suspendre Macie dans d'autres régions, répétez les étapes précédentes dans chaque région supplémentaire.

Désactiver Amazon Macie

Lorsque vous désactivez Amazon Macie, Macie cesse d'effectuer toutes les activités liées à votre compte dans leRégion AWS. Cela inclut la surveillance de vos données Amazon Simple Storage Service (Amazon S3), la découverte automatique de données sensibles et l'exécution de toutes les tâches de découverte de données sensibles actuellement en cours. Macie supprime également tous les paramètres et ressources existants qu'elle stocke ou gère pour votre compte dans la région concernée, y compris vos résultats et les tâches de découverte de données sensibles. Données que vous avez stockées ou publiées sur d'autresServices AWSreste intact et n'est pas affecté. Par exemple, les résultats de la découverte de données sensibles dans Amazon S3 et la recherche d'événements dans AmazonEventBridge.

> **Warning**
>
> Si vous désactivez Macie, vous supprimez également définitivement toutes vos découvertes existantes, vos tâches de découverte de données sensibles, vos identifiants de données personnalisés et les autres ressources que Macie stocke ou gère pour votre compte

dans la région concernée. Ces ressources ne peuvent pas être récupérées après leur suppression. Pour conserver les ressources et uniquement suspendre votre utilisation de Macie, suspendez Macie au lieu de la désactiver.

Cette rubrique explique comment désactiver Macie à l'aide de la console Amazon Macie. Si vous préférez le faire par programmation, vous pouvez utiliserDisableMaciefonctionnement de l'API Amazon Macie.

> **Note**
>
> Si votre compte fait partie d'une organisation qui gère de manière centralisée plusieurs comptes Macie, vous devez effectuer les opérations suivantes avant de désactiver Macie :
>
> - Si votre compte est un compte de membre Macie, demandez à votre administrateur Macie de le supprimer en tant que compte de membre.
> - Si votre compte est un compte administrateur Macie, supprimez tous les comptes membres associés à votre compte et supprimez les associations entre votre compte et ces comptes.
>
> La façon dont vous effectuez les tâches précédentes varie selon que votre compte Macie est associé à d'autres comptes viaAWS Organizationsou sur invitation. Pour plus d'informations, veuillez consulter Gestion de plusieurs comptes .

Pour désactiver Macie

1. Ouvrez la console Amazon Macie à l'adressehttps://console.aws.amazon.com/macie/.
2. En utilisant leRégion AWSdans le coin supérieur droit de la page, sélectionnez la région dans laquelle vous souhaitez désactiver Macie.
3. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
4. ChoisissezDésactiver Macie.
5. Lorsque vous êtes invité à confirmer, entrez**`Disable`**, puis choisissezDésactiver.

Pour désactiver Macie dans d'autres régions, répétez les étapes précédentes dans chaque région supplémentaire.

Quotas Amazon Macie

Vous Compte AWS disposez de certains quotas par défaut, anciennement appelés limites, pour chacun d'entre euxService AWS. Ces quotas correspondent au nombre maximum de ressources de service ou d'opérations pour votre compte. Cette rubrique répertorie les quotas qui s'appliquent aux ressources et aux opérations Amazon Macie pour votre compte. Sauf indication contraire, chaque quota s'applique à votre compte dans chacune d'entre ellesRégion AWS.

Certains quotas peuvent être augmentés, mais pas tous. Pour demander l'augmentation d'un quota, utilisez la console Service Quotas. Pour savoir comment demander une augmentation, consultez la section Demander une augmentation de quota dans le Guide de l'utilisateur du Service Quotas. Si aucun quota n'est disponible sur la console Service Quotas, utilisez le formulaire d'augmentation des limites de service sur le AWS Support Center Console pour demander une augmentation du quota.

Comptes

- Comptes membres sur invitation : 1 000
- Comptes membres via AWS Organizations : 10 000

Conclusions

- Règles de filtrage et règles de suppression par compte : 1 000
- Résultats par cycle d'une tâche de découverte de données sensibles : 100 000 + 5 % des résultats restants une fois le seuil de 100 000 atteint

  Ce quota s'applique uniquement à la console Amazon Macie et à l'API Amazon Macie. Il n'y a pas de quota quant au nombre d'événements de recherche publiés par Macie sur Amazon EventBridge ou au nombre de résultats de découverte de données sensibles créés par Macie pour chaque exécution d'une tâche.
- Emplacements de détection par détection de données sensibles : 15
- Demandes de récupération et de divulgation d'échantillons de données sensibles provenant d'un objet Amazon S3 : 100 par jour

  Ce quota est réinitialisé toutes les 24 heures à 00:00:01 UTC+0.
- Taille d'un objet Amazon S3 pour récupérer et révéler des échantillons de données sensibles à partir de :
  - Fichier conteneur d'objets Apache Avro (.avro) : 70 Mo

- Fichier Apache Parquet (.parquet) : 100 Mo
- Fichier CSV (.csv) : 255 Mo
- Fichier d'archive compressé GNU Zip (.gz ou .gzip) : 90 Mo
- Fichier JSON ou lignes JSON (.json ou .jsonl) : 25 Mo
- Fichier de classeur Microsoft Excel (.xlsx) : 20 Mo
- Fichier texte non binaire (text/plain) : 100 Mo
- Fichier TSV (.tsv) : 75 Mo
- Fichier d'archive compressé ZIP (.zip) : 355 Mo

Si un résultat s'applique à un fichier d'archive qui génère plusieurs fichiers .gz pour les résultats de découverte de données sensibles correspondants, les échantillons de données sensibles ne peuvent pas être récupérés et révélés à partir du fichier d'archive.

Découverte de données sensibles

- Analyse mensuelle par compte pour les tâches de découverte de données sensibles : 5 To

  Ce quota s'applique uniquement aux tâches de découverte de données sensibles. Pour augmenter le quota jusqu'à 1 000 To (1 Po), utilisez la console Service Quotas. Pour demander une augmentation de plus de 1 Po, utilisez le formulaire d'augmentation des limites de service sur leAWS Support Center Console.
- Identifiants de données personnalisés par compte : 10 000
- Autoriser les listes par compte : 10, 1 à 5 autorisent les listes qui spécifient du texte prédéfini et 1 à 5 autorisent les listes qui spécifient des expressions régulières

  Des quotas supplémentaires s'appliquent à une liste d'autorisation qui spécifie un texte prédéfini. La liste ne peut pas contenir plus de 100 000 entrées et la taille de stockage de la liste ne doit pas dépasser 35 Mo.
- Compartiments S3 à exclure de la découverte automatique des données sensibles : 1 000

  Si votre compte est le compte administrateur Macie d'une organisation, ce quota s'applique à l'ensemble de votre organisation.
- compartiments S3 par tâche de découverte de données sensibles : 1 000

  Ce quota ne s'applique pas aux tâches qui utilisent les critères d'exécution des compartiments pour déterminer les compartiments à analyser. Cela s'applique à une tâche uniquement si vous

configurez la tâche pour analyser des compartiments spécifiques que vous sélectionnez. Si votre compte est le compte administrateur Macie d'une organisation, vous pouvez sélectionner jusqu'à 1 000 compartiments couvrant jusqu'à 1 000 comptes au sein de votre organisation.

- Identifiants de données personnalisés par tâche de découverte de données sensibles : 30
- Autoriser les listes par tâche de découverte de données sensibles : 10, 1 à 5 autorisent les listes qui spécifient du texte prédéfini et 1 à 5 autorisent les listes qui spécifient des expressions régulières
- CreateClassificationJobopération : 0,1 demande par seconde
- Temps d'analyse d'un dossier individuel : 10 heures
- Taille d'un fichier individuel à analyser :
  - Fichier Adobe Portable Document Format (.pdf) : 1 024 Mo
  - Fichier conteneur d'objets Apache Avro (.avro) : 8 Go
  - Fichier Apache Parquet (.parquet) : 8 Go
  - Fichier de message électronique (.eml) : 20 Go
  - Fichier d'archive compressé GNU Zip (.gz ou .gzip) : 8 Go
  - Fichier de classeur Microsoft Excel (.xls ou .xlsx) : 512 Mo
  - Fichier de document Microsoft Word (.doc ou .docx) : 512 Mo
  - Fichier texte non binaire : 20 Go
  - Fichier d'archive TAR (.tar) : 20 Go
  - Fichier d'archive compressé ZIP (.zip) : 8 Go

  Si la taille d'un fichier est supérieure au quota applicable, Macie n'analyse aucune donnée du fichier.
- Extraction et analyse des données dans un fichier compressé ou d'archive :
  - Taille de stockage (compressée) : 8 Go pour un fichier d'archive compressée GNU Zip (.gz ou .gzip) ou un fichier d'archive compressée ZIP (.zip) ; 20 Go pour un fichier d'archive TAR (.tar)
  - Profondeur d'archivage imbriquée : 10 niveaux
  - Fichiers extraits : 1 000 000
  - Octets extraits : 10 Go de données non compressées au total. 3 Go de données non compressées pour chaque fichier extrait utilisant un type de fichier ou un format de stockage pris en charge.

Si les métadonnées d'un fichier compressé ou d'archive indiquent que le fichier contient plus de 10 niveaux imbriqués ou qu'il dépasse le quota applicable en termes de taille de stockage ou d'octets extraits, Macie n'extrait ni n'analyse aucune donnée du fichier. Si Macie commence à extraire et à analyser les données d'un fichier compressé ou d'archive et détermine par la suite que le fichier contient plus de 1 000 000 de fichiers ou dépasse le quota d'octets extraits, Macie arrête d'analyser les données du fichier et crée des résultats de découverte de données sensibles uniquement pour les données traitées.

- Analyse des éléments imbriqués dans les données structurées : 256 niveaux par fichier

  Ce quota s'applique uniquement aux fichiers JSON (.json) et JSON Lines (.jsonl). Si la profondeur imbriquée de l'un ou l'autre type de fichier dépasse ce quota, Macie n'analyse aucune donnée du fichier.
- Nombre d'emplacements de détection par résultat de découverte de données sensibles : 1 000 par type de détection de données sensibles
- Détection des noms complets : 1 000 par fichier, y compris les fichiers d'archive

  Une fois que Macie a détecté les 1 000 premières occurrences de noms complets dans un fichier, Macie arrête d'incrémenter le nombre et de communiquer les données de localisation pour les noms complets.
- Détection des adresses postales : 1 000 par fichier, y compris les fichiers d'archive

  Une fois que Macie a détecté les 1 000 premières occurrences d'adresses postales dans un fichier, Macie arrête d'augmenter le nombre d'adresses postales et de communiquer les données de localisation des adresses postales.

Historique du document pour le guide de l'utilisateur d'Amazon Macie

Le tableau suivant décrit les modifications importantes apportées à la documentation depuis la dernière version d'Amazon Macie. Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

Dernière mise à jour de la documentation : 14 juin 2024

Modification	Description	Date
Nouvelle fonction	Si vous êtes l'administrateur Macie délégué d'une organisation, vous pouvez désormais activer ou désactiver la découverte automatique des données sensibles pour les comptes individuels de votre organisation. Grâce à cette option supplémentaire, vous pouvez désormais définir la portée des analyses de plusieurs manières : activer la découverte automatique pour tous les comptes, activer la découverte automatique de manière sélective pour des comptes particuliers et exclure des compartiments S3 particuliers.	14 juin 2024
Nouvelles fonctionnalités	AWS Security Hub fournit désormais des contrôles de sécurité permettant de vérifier l'état de Macie et de détecter automatiquement les données	20 février 2024

	sensibles des comptes. Si ces contrôles sont activés, Security Hub effectue régulièrement des contrôles de sécurité pour déterminer si Macie est activé pour un Compte AWS (contrôle Macie.1) et si la découverte automatique des données sensibles est activée pour un compte Macie (contrôle Macie.2).	
Nouvelles fonctionnalités	Macie peut désormais analyser les objets Amazon S3 chiffrés à l'aide d'un chiffrement double couche côté serveur avec AWS KMS keys (DSSE-KMS). Ces objets peuvent désormais être analysés lorsque Macie effectue une découverte automatique de données sensibles ou que vous exécutez des tâches de découverte de données sensibles. En outre, les compartiments et objets S3 qui utilisent le chiffrement DSSE-KMS sont désormais inclus dans les statistiques et les métadonnées fournies par Macie concernant vos données Amazon S3.	17 janvier 2024

Nouvelle fonction	Vous pouvez désormais configurer Macie pour qu'il assume un rôle AWS Identity and Access Management (IAM) lorsque vous choisissez de récupérer et de révéler des échantillons de données sensibles que Macie rapporte dans ses conclusions. Les exemples peuvent vous aider à vérifier la nature des données sensibles découvertes par Macie et à personnaliser votre enquête sur un objet ou un compartiment Amazon S3 concernés.	16 novembre 2023
Nouvelles fonctionnalités	Macie fournit désormais des identifiants de données gérés conçus pour détecter les numéros de compte bancaire internationaux (IBAN) pour 47 pays et régions supplémentaires. Vous pouvez désormais utiliser Macie pour détecter et signaler les occurrences d'IBAN dans plus de 50 pays et régions.	1er novembre 2023

Nouvelles fonctionnalités	Macie fournit désormais des identifiants de données gérés conçus pour détecter les types de données sensibles suivants : clés d'API Google Cloud, clés d'API Stripe et numéros Aadhaar, numéros de compte permanents (PAN) et numéros d'identification de permis de conduire pour l'Inde.	25 septembre 2023
Nouveaux quotas	Pour vous aider à vérifier la nature des données sensibles signalées par les résultats , nous avons augmenté les quotas de taille pour la récupération et la divulgation d'échantillons de données sensibles provenant d'objets Amazon S3. Vous pouvez désormais récupérer et révéler des échantillons d'objets S3 dont la taille de stockage est supérieure à 10 Mo. Pour obtenir la liste des nouveaux quotas, consultez la section Quotas Amazon Macie.	7 septembre 2023

Disponibilité par région	Macie est désormais disponible dans la région Israël (Tel Aviv). Pour une liste complète des Régions AWS endroits où Macie est actuellement disponible, consultez la section Points de terminaison et quotas Amazon Macie dans le. Références générales AWS	28 août 2023
Fonctionnalités mises à jour	Nous avons mis en place un nouvel ensemble dynamique d'identifiants de données gérés par défaut pour la découverte automatisée des données sensibles. L'ensemble par défaut inclut les identifiants de données gérés que nous recommandons pour la découverte automatique de données sensibles. Il est conçu pour détecter les catégories et types courants de données sensibles tout en optimisant vos résultats de découverte automatique de données sensibles.	02/08/2023

Fonctionnalités mises à jour	Pour vous aider à localiser les occurrences de données sensibles signalées par Macie dans les résultats de découverte de données sensibles et de découvert e de données sensibles , nous avons modifié la limite de caractères de 20 à 240 pour les noms des éléments de chemin JSON dans les `Record` objets. Cette modification affecte les nouvelles découvertes de données sensibles et les résultats de découverte pour les conteneurs d'objets Apache Avro, les fichiers Apache Parquet, les fichiers JSON et les fichiers JSON Lines.	24 juillet 2023
Fonctionnalités mises à jour	Si vous êtes l'administrateur délégué de Macie pour une organisation dans AWS Organizations, vous pouvez désormais gérer Macie pour un maximum de 10 000 comptes dans votre organisat ion.	30 juin 2023

Nouvelle fonction	Vous pouvez désormais créer et configurer des tâches de découverte de données sensibles afin d'utiliser automatiquement l'ensemble d'identifiants de données gérés que nous recommandons pour les tâches. Cet ensemble recommandé d'identifiants de données gérés est conçu pour détecter les catégories et types courants de données sensibles tout en optimisant les résultats de votre travail.	28 juin 2023
Nouvelle politique	Nous avons ajouté une nouvelle politique AWS gérée, la `AmazonMacieReadOnlyAccess` politique. Cette politique accorde des autorisations en lecture seule qui permettent à une identité IAM (principal) de récupérer toutes les ressources, données et paramètres Macie de son compte.	15 juin 2023

Nouvelle fonction	Pour vous aider à évaluer et à surveiller la couverture automatisée des données sensibles de vos données Amazon S3, la console Macie inclut désormais une page de couverture des ressources. La page fournit une vue unifiée des statistiques et des données de couverture pour tous vos compartiments S3, y compris un récapitulatif des problèmes d'analyse (le cas échéant) survenus récemment pour chaque compartiment. En cas de problème, la page fournit également des conseils de résolution.	15 mai 2023
Nouvelle fonction	Macie s'intègre à Notifications des utilisateurs AWS, qui est un nouveau site Service AWS qui sert d'emplacement central pour vos AWS notifications sur le AWS Management Console. Vous pouvez ainsi configurer des Notifications des utilisateurs règles et des canaux de diffusion personnalisés pour générer et envoyer des notifications concernant les EventBridge événements Amazon publiés par Macie pour obtenir des informations sur les politiques et les données sensibles.	5 mai 2023

Contenu mis à jour	Descriptions mises à jour des statistiques et des métadonnées fournies par Macie concernant les paramètres de chiffrement par défaut pour les compartiments S3. La description des conclusions relatives à la Policy:IAMUser/S3BucketEncryptionDisabled politique a également été mise à jour. Amazon S3 applique désormais automatiquement le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) comme niveau de chiffrement de base pour les objets ajoutés aux buckets nouveaux et existants. Pour plus d'informations sur cette modification apportée à Amazon S3, consultez la section Définition du comportement de chiffrement côté serveur par défaut pour les compartiments S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.	27 février 2023

Nouvelles fonctionnalités	Macie peut désormais générer un type supplémentaire de recherche de politique pour un compartiment S3 : `Policy:IAMUser/S3BucketSharedWithCloudFront` . Ce type de résultat indique que la politique d'un compartiment a été modifiée pour autoriser le partage du compartiment avec une identité CloudFront d'accès à l'origine (OAI) Amazon, un contrôle CloudFront d'accès à l'origine (OAC), ou les deux. En outre, les buckets partagés avec des OAI ou CloudFront des OAC sont désormais considérés comme partagés en externe dans les statistiques et les métadonnées fournies par Macie concernant vos données Amazon S3.	24 février 2023

Nouvelles fonctionnalités	Macie prend désormais en charge la classe de stockage Amazon S3 Glacier Instant Retrieval pour la découverte de données sensibles. Les objets S3 qui utilisent cette classe de stockage peuvent désormais être analysés lorsque Macie effectue une découverte automatique de données sensibles ou que vous exécutez des tâches de découverte de données sensibles. Ils sont également considérés comme des objets classifiables dans les statistiques et les métadonnées que Macie fournit à propos de vos données Amazon S3.	21 décembre 2022

Nouvelle fonction	Vous pouvez désormais configurer Macie pour effectuer la découverte automatique des données sensibles pour votre compte ou votre organisation. Grâce à la découverte automatiq ue des données sensibles, Macie évalue en permanenc e vos données Amazon S3 et utilise des techniques d'échantillonnage pour identifie r, sélectionner et analyser des objets représentatifs dans vos compartiments S3, en inspectant les objets pour détecter la présence de données sensibles. Vous pouvez évaluer les résultats des analyses dans les statistiq ues, les résultats et les autres informations fournies par Macie sur vos données Amazon S3.	28 novembre 2022

Nouvelle fonction	Vous pouvez désormais créer et utiliser des listes d'autorisation pour spécifier le texte et les modèles de texte que vous souhaitez que Macie ignore lorsqu'il inspecte les objets Amazon S3 à la recherche de données sensibles. À l'aide de listes d'autorisation, vous pouvez définir des exceptions relatives aux données sensibles pour vos scénarios ou votre environnement particuliers, par exemple les noms des représentants publics de votre organisation, des numéros de téléphone spécifiques ou des exemples de données que votre organisation utilise pour les tests.	30 août 2022
Nouvelle fonction	Pour vérifier la nature des données sensibles que Macie trouve dans les objets S3, vous pouvez désormais configurer et utiliser Macie pour récupérer des échantillons de données sensibles signalées par les résultats.	26 juillet 2022

Fonctionnalités mises à jour	Dans la AmazonMacieFullAccesspolitique, nous avons mis à jour le nom de ressource Amazon (ARN) du rôle lié au service Macie (). `aws-service-role/macie.amazonaws.com/AWSServiceRoleForAmazonMacie`	30 juin 2022
Fonctionnalités mises à jour	Nous avons mis à jour la AmazonMacieServiceRolePolicypolitique, qui est la politique attachée au rôle lié au service Macie (). `AWSServiceRoleForAmazonMacie` La politique ne spécifie plus les actions et les ressources pour Amazon Macie Classic. Amazon Macie Classic n'est plus disponible et n'est plus disponible.	20 mai 2022
Nouvelles fonctionnalités	Macie inclut désormais ce `OriginType` domaine dans les résultats de données sensibles sur lesquels il publie. AWS Security Hub Le `OriginType` champ indique comment Macie a trouvé les données sensibles à l'origine du résultat.	11 mai 2022

Contenu mis à jour	Clarification du fonctionnement des paramètres des mots clés et de la distance de correspondance maximale pour les identifiants de données personnalisés.	22 avril 2022
Nouvelles fonctionnalités	Macie fournit désormais des identifiants de données gérés conçus pour détecter les en-têtes d'autorisation HTTP Basic, les cookies HTTP et les jetons Web JSON.	21 avril 2022
Nouveau contenu	Ajout de descriptions et de définitions des concepts et termes clés pour Macie.	16 mars 2022
Nouvelles fonctionnalités	Pour calculer et afficher les coûts estimés lorsque vous créez et configurez des tâches de découverte de données sensibles, Macie récupère désormais les données de tarification pour vous Compte AWS auprès de. AWS Billing and Cost Management Pour prendre en charge cette fonctionnalité, nous avons ajouté une action Billing and Cost Management à la AmazonMacieFullAccesspolitique.	7 mars 2022

Nouvelles fonctionnalités	Macie inclut désormais le `Sample` domaine dans les résultats qu'il publie. AWS Security Hub Le `Sample` champ indique si un résultat est un échantillon de résultat.	24 février 2022
Nouveau contenu	Ajout d'informations sur l'utilisation d'Amazon Virtual Private Cloud pour établir une connexion privée entre votre VPC et Macie.	19 janvier 2022
Nouvelles fonctionnalités	Vous pouvez désormais utiliser la console Amazon Macie pour attribuer et gérer des balises pour des identifiants de données personnalisés, des règles de filtrage et de suppression pour les résultats, des tâches de découverte de données sensibles et, si vous êtes l'administrateur Macie d'une organisation, les comptes des membres de votre organisation. Une balise est une étiquette que vous pouvez éventuellement définir et attribuer à certains types de AWS ressources.	12 janvier 2022
Nouveau contenu	Ajout d'informations sur l'utilisation AWS Identity and Access Management pour gérer l'accès à Macie.	20 décembre 2021

Nouvelle fonction	Lorsque vous créez un identifiant de données personnalisé, vous pouvez désormais définir des paramètres de gravité pour les résultats de données sensibles qu'il produit. Avec ces paramètres, vous pouvez spécifier la sévérité à attribuer à un résultat en fonction du nombre d'occurrences de texte correspondant aux critères de détection de l'identifiant de données personnalisé.	4 novembre 2021
Nouvelles fonctionnalités	Pour en savoir plus sur les différents types de résultats fournis par Macie, vous pouvez générer des exemples de résultats. Les exemples de résultats utilisent des exemples de données et des valeurs d'espace réservé pour démontrer le type d'informations que Macie peut inclure dans chaque type de résultat.	28 octobre 2021
Nouvelles fonctionnalités	Macie inclut désormais le `OwnerAccountId` domaine dans les résultats qu'il publie. AWS Security Hub Ce champ indique l'ID de compte du Compte AWS propriétaire du compartiment S3 concerné.	27 octobre 2021

Nouveau contenu	Ajout d'informations sur la gestion centralisée de plusieurs comptes Macie. Vous pouvez le faire de deux manières : en intégrant Macie à Macie AWS Organizations ou en envoyant des invitations d'adhésion depuis Macie.	13 octobre 2021
Nouvelles fonctionnalités	L'inventaire de votre compartiment S3 indique désormais si les paramètres d'autorisation d'un compartim ent empêchent Macie de récupérer des informations sur le compartiment ou les objets du compartiment et d'évaluer et de surveiller la sécurité et la confidentialité des données du compartiment. En outre, nous avons mis à jour les références AWS KMS keys et les clés gérées par le client afin de refléter la terminologie actuelle.	5 octobre 2021

Nouvelles fonctionnalités	Macie conserve désormais les informations relatives aux politiques et aux données sensibles pendant 90 jours au lieu de 30 jours. Si Macie a créé ou mis à jour un résultat le 31 août 2021 ou après cette date, vous pouvez accéder au résultat pendant 90 jours au maximum à l'aide de la console Macie ou de l'API Macie. Dans certains Régions AWS cas, Macie a commencé à conserver les résultats pendant 90 jours dès le 27 septembre 2021.	1er octobre 2021
Nouvelle fonction	Lorsque vous créez une tâche de découverte de données sensibles, vous pouvez désormais spécifier les identifiants de données gérées que vous souhaitez que la tâche utilise lorsqu'elle analyse des objets S3. Grâce à cette fonctionnalité, vous pouvez personnaliser l'analyse d'une tâche pour vous concentrer sur certains types de données sensibles.	17 septembre 2021

Nouvelles fonctionnalités	Les résultats relatifs aux données sensibles fournissent désormais des informations supplémentaires pour vous aider à localiser les données sensibles dans les fichiers JSON et JSON Lines.	6 juillet 2021
Fonctionnalités mises à jour	Macie utilise désormais le type de `AwsS3Bucket` ressource dans les résultats sur lesquels il publie. AWS Security Hub(Macie avait précédemment défini cette valeur sur`AWS::S3::Bucket` .) `AwsS3Bucket` est la valeur du type de ressource utilisée pour les compartiments S3 au format ASFF (AWS Security Finding Format).	28 juin 2021
Nouvelle fonction	Lorsque vous créez une tâche de découverte de données sensibles, vous pouvez désormais définir des critères d'exécution qui détermine nt les compartiments S3 analysés par la tâche. Grâce à cette fonctionnalité, l'étendue de l'analyse d'une tâche peut s'adapter de manière dynamique aux modifications apportées à votre inventaire de compartiments.	15 mai 2021

Nouvelles fonctionnalités	Votre inventaire de compartiments S3 et le tableau de bord récapitulatif fournissent désormais des métadonnées de chiffrement et des statistiques indiquant si les politiques relatives aux compartiments nécessitent le chiffrement côté serveur des nouveaux objets. En outre, vous pouvez désormais actualiser à la demande les métadonnées des objets pour les compartiments individuels de votre inventaire de compartiments.	30 avril 2021
Nouvelle fonction	Vous pouvez désormais utiliser Amazon CloudWatch Logs pour surveiller et analyser les événements qui se produisent lorsque vous exécutez des tâches de découverte de données sensibles. Pour prendre en charge cette fonctionnalité, nous avons ajouté CloudWatch des actions Logs à la politique AWS gérée pour le rôle lié au service Macie.	14 avril 2021
Disponibilité par région	Macie est désormais disponible dans la région AWS Asie-Pacifique (Osaka).	5 avril 2021

Nouvelle fonction	Vous pouvez désormais configurer Macie pour publier les résultats de données sensibles sur AWS Security Hub.	22 mars 2021
Nouveau contenu	Ajout d'informations sur le suivi et la prévision des coûts de Macie et sur la participation à l'essai gratuit.	26 février 2021
Contenu mis à jour	Nous avons remplacé le terme compte principal par le terme compte administrateur. Un compte administrateur est utilisé pour gérer plusieurs comptes de manière centralisée.	12 février 2021
Nouvelles fonctionnalités	Vous pouvez désormais affiner la portée des tâches de découverte de données sensibles en utilisant les préfixes d'objets S3 dans les critères d'inclusion et d'exclusion personnalisés.	2 février 2021
Contenu mis à jour	Macie adhère désormais à la taxonomie des types de recherche du AWS Security Finding Format (ASFF) lorsqu'il publie les résultats des politiques sur. AWS Security Hub	28 janvier 2021

Nouveau contenu	Ajout d'informations sur la surveillance des données Amazon S3 et l'évaluation de la sécurité et de la confidentialité de ces données.	8 janvier 2021
Disponibilité par région	Macie est désormais disponible dans les régions AWS Afrique (Le Cap), AWS Europe (Milan) et AWS Moyen-Orient (Bahreïn).	21 décembre 2020
Nouvelles fonctionnalités	Si votre compte est un compte administrateur Macie, vous pouvez désormais créer et exécuter des tâches de découverte de données sensibles qui analysent les données de 1 000 compartiments couvrant jusqu'à 1 000 comptes au sein de votre organisation.	25 novembre 2020
Nouvelles fonctionnalités	L'inventaire de votre compartiment S3 indique désormais si vous avez configuré des tâches ponctuelles ou périodiques de découverte de données sensibles pour analyser les données d'un compartiment. Si c'est le cas, il fournit également des détails sur la tâche exécutée le plus récemment.	23 novembre 2020

Nouveau contenu	Ajout d'informations sur le filtrage des résultats.	12 novembre 2020
Nouvelles fonctionnalités	Les résultats relatifs aux données sensibles fournissent désormais des informations supplémentaires pour vous aider à localiser les données sensibles dans les conteneurs d'objets Apache Avro, les fichiers Apache Parquet et les classeurs Microsoft Excel.	9 novembre 2020
Nouvelle fonction	Vous pouvez désormais utiliser les résultats de données sensibles pour localiser des occurrences individuelles de données sensibles dans des objets S3.	22 octobre 2020
Nouvelle fonction	Vous pouvez désormais suspendre et reprendre les tâches de découverte de données sensibles.	16 octobre 2020
Nouveau contenu	Ajout de détails sur le système de notation de gravité pour les conclusions relatives aux politiques et les conclusions relatives aux données sensibles.	6 octobre 2020

Nouvelles fonctionnalités	Vous pouvez désormais consulter les statistiques qui indiquent la quantité de données que Macie peut analyser dans des compartiments S3 individuels lorsque vous exécutez une tâche de découverte de données sensibles. En outre, vous pouvez désormais consulter le coût estimé d'une tâche lorsque vous créez une tâche.	3 septembre 2020
Nouveau contenu	Ajout d'informations sur la configuration, l'exécution et la gestion des tâches de découverte de données sensibles.	31 août 2020
Nouvelles fonctionnalités	Les identifiants de données gérés peuvent désormais détecter certains types d'informations personnelles identifiables pour le Brésil.	31 juillet 2020
Contenu mis à jour	Ajout d'informations sur la syntaxe prise en charge pour les expressions régulières dans les identificateurs de données personnalisés.	30 juillet 2020

Contenu mis à jour	Ajout d'exigences relatives aux mots clés pour les identificateurs de données gérés et augmentation du quota du nombre de résultats que chaque tâche de découverte de données sensibles peut produire.	17 juillet 2020
Nouveau contenu	Ajout d'informations sur l'utilisation d'Amazon EventBridge et sur AWS Security Hub le suivi et le traitement des résultats. Cela inclut le schéma des EventBridge événements pour les résultats et des exemples d'événements pour les conclusions relatives aux politiques et aux données sensibles.	22 juin 2020
Nouveau contenu	Ajout d'informations sur l'analyse et la suppression de résultats.	17 juin 2020
Nouveau contenu	Ajout d'instructions pour configurer Macie afin de stocker les résultats de découverte détaillés dans un compartiment S3.	2 juin 2020
Nouveau contenu	Ajout d'informations sur les types de données sensibles que Macie peut détecter et les exigences de chiffrement pour détecter les données sensibles dans les objets Amazon S3.	28 mai 2020

Disponibilité générale	Il s'agit de la première version publique du guide de l'utilisateur Amazon Macie.	13 mai 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.