aws

Guide de l’utilisateur

Amazon Detective

Amazon Detective: Guide de l’utilisateur

Table of Contents

Qu'est-ce que Detective ? 1
Caractéristiques d'Amazon Detective 1
Accès à Amazon Detective 3
Tarification d'Amazon Detective 5
Fonctionnement de Detective 5
Qui utilise Detective ? 6
Services connexes 7
Concepts et terminologie 9
Premiers pas 14
Configuration 14
Inscrivez-vous pour un Compte AWS 15
Création d'un utilisateur doté d'un accès administratif 15
Prérequis 17
Octroi des autorisations Detective requises 17
AWS Command Line Interface Version prise en charge 17
Recommandations 17
Alignement recommandé avec GuardDuty et AWS Security Hub 17
Mise à jour recommandée de la fréquence des GuardDuty CloudWatch notifications 18
Activation de Detective 19
Vérifier que Detective ingère des données 21
Données dans un graphe de comportement 22
Comment Detective remplit un graphique de comportement 23
Comment Detective traite les données sources 23
Extraction de Detective 24
Analyse Detective 24
Période de formation pour les nouveaux graphes de comportement 24
Vue d'ensemble de la structure de données du graphe de comportement 25
Types d'éléments dans la structure de données du graphe de comportement 25
Types d'entités dans la structure de données du graphe de comportement 26
Données source utilisées dans un graphe de comportement 32
Types de sources de données principales dans Detective 32
Types de sources de données facultatives dans Detective 33
Journaux EKS d'audit Amazon 34
AWS constatations relatives à la sécurité 35

Comment Detective ingère et stocke les données sources 36
Comment Detective applique le quota de volume de données pour les graphes de comportement 37
Tableau de bord récapitulatif 39
Enquêtes 40
Géolocalisations nouvellement observées 40
Groupes de résultats actifs au cours des 7 derniers jours 41
Rôles et utilisateurs ayant le plus grand volume API d'appels 41
EC2instances avec le volume de trafic le plus élevé 42
Clusters de conteneurs avec le plus grand nombre de pods Kubernetes 42
Notification de valeur approximative 43
Comment Detective est utilisé pour les enquêtes 44
Phases de l'enquête 44
Points de départ d'une enquête Detective 45
Résultats détectés par GuardDuty 45
AWS résultats de sécurité agrégés par Security Hub 45
Entités extraites des données source de Detective 46
Flux Detective Investigation 46
Detective Investigation 48
Mener une enquête Detective 48
Révision des rapports de Detective Investigations 51
Comprendre un rapport de Detective Investigations 52
Résumé du rapport Detective Investigations 54
Téléchargement d'un rapport de Detective Investigations 54
Archivage d'un rapport de Detective Investigations 55
Analyse des résultats 57
Vue d'ensemble des résultats 58
Durée de validité prise en compte pour la vue d'ensemble des résultats 58
Détails d'un résultat 58
Entités associées 58
Résolution des problèmes liés au message « Page introuvable » 58
Trouver des groupes 59
Comprendre la page de groupes de résultats 61
Résultats informatifs dans les groupes de résultats 63
Profils de groupes de résultats 64
Visualisation de groupe de résultats 66

Récapitulatif des groupes de résultats 69
Examen du récapitulatif du groupe de résultats 69
Désactivation du récapitulatif des groupes de résultats 71
Activation du récapitulatif des groupes de résultats 72
Régions prises en charge 72
Archivage d'une découverte GuardDuty 72
Analyse des entités 74
Utilisation de profils d'entités 74
Durée de validité d'un profil d'entité 75
Identifiant et type d'entité 75
Résultats impliqués 75
Groupes de résultats impliquant cette entité 75
Volets de profil contenant les détails des entités et les résultats d'analyse 76
Naviguer dans un profil d'entité 76
Panneaux profilés 77
Types d'informations sur un volet de profil 77
Types de visualisations du volet de profil 81
Préférences pour les volets de profil 86
Accéder au profil d'une entité 87
Pivotement depuis une autre console 88
Navigation à l'aide d'une URL 90
Ajout d'URL Detective pour les résultats dans Splunk 94
Basculement vers une autre console 94
Basculement vers un autre profil d'entité 94
Exploration des détails d'activité 95
Volume global API d'appels 96
Géolocalisations 104
Volume VPC de débit global 108
Volume global d'appels Kubernetes API 113
Gestion de la durée de validité 117
Définition de dates et d'heures de début et de fin spécifiques 118
Modifier la durée de validité 118
Réglage de la durée de validité sur une fenêtre temporelle de résultats 119
Réglage de la durée de validité sur la page de résumé 119
Affichage des résultats d'une entité 120
Entité à volume élevé 121

Qu'est-ce qu'une entité à volume élevé ? 121
Affichage de notification d'entité à volume élevé sur un profil 121
Affichage de la liste des entités à volume élevé pour la durée de validité actuelle 122
Recherche d'un résultat ou d'une entité 124
Finalisation de la recherche 124
Utilisation des résultats de recherche 126
Résolution des problèmes liés à la recherche 126
Gestion des comptes 128
Limites et recommandations 129
Nombre maximal de comptes membres 129
Comptes et régions 129
Alignement des comptes d'administrateur avec Security Hub et GuardDuty 130
Octroi des autorisations requises pour les comptes administrateurs 130
Faire apparaître les mises à jour de l'organisation dans Detective 130
Utilisation des Organisations pour gérer les comptes de graphes comportementaux 130
Désignez un compte administrateur Detective pour votre organisation 131
Activer les comptes de l'organisation en tant que comptes membres 132
Désignation du compte administrateur Detective 133
Désignation d'un administrateur Detective 134
Suppression du compte administrateur Detective 137
Actions disponibles pour les comptes 140
Consulter la liste des comptes 142
Listing des comptes (console) 143
Répertorier vos comptes de membres (DetectiveAPI, AWS CLI) 145
Gestion des comptes membres de l'organisation 146
Activation de nouveaux comptes d'organisation 147
Activation des comptes d'organisation en tant que comptes membres de Detective 149
Dissociation des comptes de l'organisation 150
Gestion des comptes membres 152
Inviter des comptes individuels à accéder à un graphique de comportement 154
Inviter une liste de comptes membres à un graphique de comportement 156
Activation d'un compte membre non activé 157
Supprimer des comptes de membres 159
Pour les comptes membres : gestion des invitations et des appartenances 160
IAMpolitique relative à un compte de membre 161
Afficher les invitations à des graphes de comportement 162

Réponse à une invitation de graphe de comportement 164
Supprimer votre compte d'un graphe de comportement 165
Effet des actions du compte 166
Detective désactivé 167
Le compte membre a été supprimé du graphe de comportement 167
Le compte membre quitte l'organisation 167
AWS compte suspendu 167
AWS compte fermé 168
Scripts Python d'Amazon Detective 168
Vue d'ensemble du script `enableDetective.py` 169
Vue d'ensemble du script `disableDetective.py` 170
Autorisations requises pour les scripts 170
Configuration de l'environnement d'exécution pour les scripts Python 171
Création d'une liste `.csv` de comptes membres à ajouter ou à supprimer 173
Exécution d'`enableDetective.py` 174
Exécution d'`disableDetective.py` 175
Detective Integration avec Security Lake 177
Activation de l'intégration 177
Avant de commencer 179
Étape 1 : Création d'un abonné Security Lake dans Detective 179
Étape 2 : ajout des autorisations IAM requises 180
Étape 3 : Acceptation de l'invitation Resource Share ARN 183
Modification de la configuration de l'intégration de Detective 190
AWS Régions prises en charge 191
Interrogation des journaux bruts dans Detective 193
Interrogation de logs bruts pour un rôle AWS 196
Interrogation de journaux bruts pour un cluster Amazon EKS 196
Interrogation de logs bruts pour une instance Amazon EC2 197
Désactivation de l'intégration 197
Supprimer une CloudFormation pile 198
Prévision et surveillance des coûts 200
À propos de la version d'essai gratuite des graphes de comportement 200
Essai gratuit pour les sources de données facultatives 201
Utilisation et coûts du compte administrateur 202
Volume de données ingérées pour chaque compte 202
Coûts prévus pour le graphe de comportement 203

Coût prévu pour le graphe de comportement ... 203
Volume de données ingérées par les packages sources ... 203
Suivi de l'utilisation du compte membre ... 204
Volume ingéré pour chaque graphe de comportement ... 204
Coût projeté sur la base de graphes de comportement ... 205
Comment Amazon Detective calcule le coût prévisionnel ... 205
Sécurité ... 207
Protection des données ... 208
Gestion des clés ... 209
Gestion des identités et des accès ... 209
Public ciblé ... 210
Authentification avec des identités ... 210
Gestion des accès à l'aide de politiques ... 214
Comment Amazon Detective travaille avec IAM ... 217
Exemples de politiques basées sur l'identité ... 224
AWS politiques gérées ... 230
Utilisation des rôles liés à un service ... 241
Résolution des problèmes d'identité et d'accès ... 243
Validation de conformité ... 245
Résilience ... 246
Sécurité de l'infrastructure ... 247
Bonnes pratiques de sécurité ... 247
Bonnes pratiques pour les comptes d'administrateur de Detective ... 247
Bonnes pratiques relatives aux comptes membres ... 248
Enregistrement API des appels ... 249
Informations de détective dans CloudTrail ... 249
Vue d'ensemble des entrées du fichier journal de Detective ... 250
Régions et quotas ... 252
Régions et points de terminaison de Detective ... 252
Quotas de Detective ... 252
Internet Explorer 11 n'est pas pris en charge ... 253
Gestion des balises ... 254
Afficher les balises d'un graphe de comportement ... 254
Ajouter des balises à un graphe de comportement ... 255
Supprimer des balises d'un graphe de comportement ... 256
Désactivation Amazon Detective ... 257

Désactiver Detective (console) 257
Désactiver Detective (Detective API, AWS CLI) 257
Désactiver Detective across Regions (script Python activé GitHub) 258
Historique de la documentation 259
..... ccxci

Présentation d'Amazon Detective

Amazon Detective vous permet d'analyser, d'enquêter et d'identifier rapidement la cause à l'origine des résultats de sécurité ou des activités suspectes. Detective collecte automatiquement les données des journaux à partir de vos ressources AWS . Detective utilise ensuite le machine learning, l'analyse statistique et la théorie des graphes pour générer des visualisations qui vous aideront à mener des investigations de sécurité plus rapides et plus efficaces. Les agrégations de données, les résumés et le contexte prédéfinis de Detective vous aident à analyser et à déterminer rapidement la nature et l'étendue des éventuels problèmes de sécurité.

Avec Detective, vous pouvez accéder à un an de données historiques sur les événements. Ces données sont disponibles via un ensemble de visualisations qui montrent l'évolution du type et du volume d'activité au cours d'une période sélectionnée. Detective associe ces changements aux GuardDuty découvertes. Pour plus d'informations sur les sources de données, consultez the section called "Données source utilisées dans un graphe de comportement".

En agrégeant automatiquement les données et en fournissant des outils visuels, Amazon Detective vous permet de mener des enquêtes de sécurité plus rapides et plus efficaces. Vous pouvez rapidement analyser les problèmes potentiels et déterminer l'ampleur des menaces de sécurité.

Rubriques

- Caractéristiques d'Amazon Detective
- Accès à Amazon Detective
- Tarification d'Amazon Detective
- Fonctionnement de Detective
- Qui utilise Detective ?
- Services connexes

Caractéristiques d'Amazon Detective

Voici quelques-unes des principales fonctionnalités d'Amazon Detective pour enquêter sur les activités suspectes dans votre AWS environnement et analyser les ressources afin d'identifier la cause première des problèmes de sécurité.

Detective trouve des groupes

Les groupes Detective Finding vous permettent d'examiner plusieurs activités liées à un événement de sécurité potentiel. Vous pouvez analyser la cause première des GuardDuty résultats très graves à l'aide de groupes de recherche. Si un auteur de menaces tente de compromettre votre AWS environnement, il exécute généralement une séquence d'actions qui génèrent de multiples résultats de sécurité et des comportements inhabituels.

La page des groupes de recherche de Detective affiche tous les groupes de recherche associés extraits de votre graphe de comportement. Pour plus d'informations sur la manière dont vous pouvez tirer parti des groupes de recherche pour analyser la cause première des résultats de sécurité, consultez la section Analyse des groupes de recherche dans Detective.

Detective fournit une visualisation interactive de chaque groupe de recherche pour vous aider à étudier les problèmes de sécurité plus rapidement et de manière plus approfondie. La visualisation est conçue pour afficher les entités et les résultats impliqués dans un incident de sécurité, ce qui facilite la compréhension des connexions et des causes profondes. Elle vous aide à étudier les problèmes plus rapidement et de manière plus approfondie avec moins d'efforts. Le panneau de visualisation du groupe de recherche affiche les résultats et les entités impliquées dans un groupe de recherche.

Detective Investigation pour trier les résultats

Avec Detective Investigation, vous pouvez enquêter sur IAM les utilisateurs et les IAM rôles à l'aide d'indicateurs de compromission, qui peuvent vous aider à déterminer si une ressource est impliquée dans un incident de sécurité. Un indicateur de compromission (IOC) est un artefact observé dans ou sur un réseau, un système ou un environnement qui peut (avec un niveau de confiance élevé) identifier une activité malveillante ou un incident de sécurité. Avec Detective investigations, vous pouvez optimiser l'efficacité, vous concentrer sur les menaces de sécurité et renforcer les capacités de réponse aux incidents.

Detective Investigation utilise des modèles d'apprentissage automatique et des informations sur les menaces pour détecter uniquement les problèmes les plus critiques et les plus suspects, vous permettant ainsi de vous concentrer sur des enquêtes de haut niveau. Il analyse automatiquement les ressources de votre AWS environnement afin d'identifier les indicateurs potentiels de compromission ou d'activité suspecte. Cela vous permet d'identifier les modèles et de comprendre quelles ressources sont affectées par les événements de sécurité, offrant ainsi une approche proactive de l'identification et de l'atténuation des menaces.

Vous pouvez utiliser Start a Detective Investigation depuis la console Detective en exécutant une enquête Detective. Pour exécuter une enquête par programmation, utilisez le StartInvestigationDetective. API Pour exécuter une enquête à l'aide de la AWS Command Line Interface (AWS CLI), exécutez la commande start-investigation.

Intégration de Detective à Amazon Security Lake

Detective s'intègre à Amazon Security Lake, ce qui signifie que vous pouvez interroger et récupérer les données de journal brutes stockées par Security Lake. Grâce à cette intégration, vous pouvez collecter des journaux et des événements à partir des sources suivantes, prises en charge de manière native par Security Lake.

- AWS CloudTrail événements de gestion version 1.0 et versions ultérieures
- Amazon Virtual Private Cloud (AmazonVPC) Flow Logs version 1.0 et ultérieure
- Journal d'audit Amazon Elastic Kubernetes Service (EKSAmazon) version 2.0

Après avoir intégré Detective à Security Lake, Detective commence à extraire les logs bruts de Security Lake relatifs aux événements AWS CloudTrail de gestion et à Amazon VPC Flow Logs. Vous pouvez interroger les journaux bruts pour consulter les journaux et les événements dans Detective.

Étudier VPC le volume de débit

Avec Detective, vous pouvez examiner de manière interactive les détails de l'activité des flux réseau de cloud privé virtuel (VPC) de vos instances Amazon Elastic Compute Cloud (AmazonEC2) et de vos pods Kubernetes. Detective collecte automatiquement les journaux de VPC flux de vos comptes surveillés, les agrège par EC2 instance et présente des résumés visuels et des analyses sur ces flux réseau.

Pour une EC2 instance, les détails de l'activité pour le volume de VPC flux global indiquent les interactions entre l'EC2instance et les adresses IP pendant une période sélectionnée.

Pour un pod Kubernetes, le volume de VPC flux global affiche le volume global d'octets entrant et sortant de l'adresse IP attribuée au pod Kubernetes pour toutes les adresses IP de destination.

Accès à Amazon Detective

Amazon Detective est disponible dans la plupart des cas Régions AWS. Pour obtenir la liste des régions dans lesquelles Detective est actuellement disponible, consultez la section Points

de terminaison et quotas Amazon Detective 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 Gestion de compte AWS référence.

Dans chaque région, vous pouvez travailler avec Detective 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 Detective permet d'accéder à votre compte Detective, à vos données et à vos ressources. Vous pouvez effectuer n'importe quelle tâche de Detective à l'aide de la console Detective : passez en revue les menaces de sécurité potentielles et analysez, étudiez et identifiez la cause première des découvertes de sécurité.

AWS outils de ligne de commande

Grâce aux outils de ligne de AWS commande, vous pouvez émettre des commandes sur la ligne de commande de votre système pour exécuter des tâches et AWS des tâches de Detective. 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 Outils AWS pour 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 Outils AWS pour PowerShell l'utilisateur.

AWS SDKs

AWS fournit SDKs des bibliothèques et des exemples de code pour divers langages de programmation et plateformes, par exemple Java, Go, Python, C++ et. NET. Ils SDKs fournissent un accès pratique et programmatique à Detective 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 du AWS SDKs, voir Outils sur lesquels s'appuyer AWS.

Amazon Detective REST API

Amazon Detective vous REST API donne un accès complet et programmatique à votre compte Detective, à vos données et à vos ressources. Vous pouvez API ainsi envoyer des HTTPS

demandes directement à Detective. Cependant, contrairement aux outils de ligne de AWS commandeSDKs, leur utilisation 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 à ce sujetAPI, consultez le Detective API Reference.

Tarification d'Amazon Detective

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

La tarification de Detective repose sur plusieurs critères et facture un tarif forfaitaire échelonné par Go pour toutes les données, quelle que soit leur source. Pour plus d'informations, consultez les tarifs d'Amazon Detective.

Pour vous aider à comprendre et à prévoir le coût d'utilisation de Detective, Detective fournit une estimation des coûts d'utilisation de votre compte. Vous pouvez consulter ces estimations sur la console Amazon Detective et y accéder avec Amazon DetectiveAPI. Selon la manière dont vous utilisez le service, l'utilisation d'autres Services AWS fonctionnalités associées à certaines fonctionnalités de Detective, telles que l'intégration de Security Lake et Detective Investigations, peut entraîner des coûts supplémentaires.

Lorsque vous activez Detective pour la première fois, vous êtes automatiquement Compte AWS inscrit à l'essai gratuit de 30 jours de Detective. Cela inclut les comptes individuels activés dans le cadre d'une organisation dans AWS Organizations. Pendant l'essai gratuit, l'utilisation de Detective dans la version applicable est gratuite Région AWS.

Pour vous aider à comprendre et à prévoir le coût d'utilisation de Detective après la fin de l'essai gratuit, Detective vous fournit une estimation des coûts d'utilisation en fonction de votre utilisation de Detective 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 les données relatives à l'utilisation de votre compte Detective sur la console Amazon Detective et y accéder avec Amazon DetectiveAPI.

Fonctionnement de Detective

Detective extrait automatiquement les événements temporels tels que les tentatives de connexion, API les appels et le trafic réseau depuis les journaux de VPC flux Amazon AWS CloudTrail et Amazon. Il ingère également les résultats détectés par GuardDuty.

À partir de ces événements, Detective utilise le machine learning et la visualisation pour créer une vue unifiée et interactive du comportement de vos ressources et de leurs interactions au fil du temps. Vous pouvez explorer ce graphique de comportement pour examiner des actions disparates telles que des tentatives d'ouverture de session infructueuses ou des appels suspectsAPI. Vous pouvez également voir comment ces actions affectent les ressources telles que les AWS comptes et les EC2 instances Amazon. Vous pouvez ajuster la validité et la chronologie du graphe de comportement pour diverses tâches :

- Étudier rapidement toute activité qui sort de la norme.
- Identifier les modèles susceptibles d'indiquer un problème de sécurité.
- Comprendre toutes les ressources affectées par un résultat.

Les visualisations personnalisées de Detective fournissent une base de référence et résument les informations du compte. Ces résultats peuvent aider à répondre à des questions telles que « Est-ce un API appel inhabituel pour ce rôle ? » Ou « Ce pic de trafic provenant de cette instance est-il attendu ? »

Avec Detective, il n'est plus nécessaire d'organiser les données ni de développer, de configurer ou d'ajuster les requêtes et les algorithmes. Il n'y a pas de frais initiaux et vous ne payez que les événements analysés, sans logiciel supplémentaire à déployer ou à d'autres flux auxquels s'abonner.

Qui utilise Detective ?

Lorsqu'un compte active Detective, il devient le compte administrateur d'un graphe de comportement. Un graphe de comportement est un ensemble lié de données extraites et analysées à partir d'un ou de plusieurs AWS comptes. Les comptes administrateurs peuvent ensuite inviter d'autres comptes membres à fournir leurs données au graphe de comportement.

Detective est également intégré à AWS Organizations. Le compte de gestion de votre organisation désigne un compte administrateur Detective pour l'organisation. Le compte administrateur Detective active les comptes d'organisation en tant que comptes membres dans le graphe de comportement de l'organisation.

Pour plus d'informations sur la manière dont Detective utilise les données source des comptes de graphes comportementaux, consultez the section called "Données source utilisées dans un graphe de comportement".

Pour plus d'informations sur la manière dont les comptes administrateurs gèrent les graphes de comportement, consultez Gestion des comptes. Pour plus d'informations sur la manière dont les comptes membres gèrent leur comportement, les invitations graphes et les adhésions, consultez the section called "Pour les comptes membres : gestion des invitations et des appartenances".

Le compte administrateur utilise les analyses et les visualisations générées à partir du graphe de comportement pour étudier les AWS ressources et GuardDuty les résultats. Grâce aux intégrations de Detective avec GuardDuty et AWS Security Hub, vous pouvez passer d'une GuardDuty recherche dans ces services directement à la console Detective.

Une enquête Detective se concentre sur l'activité liée aux ressources AWS impliquées. Pour une présentation du processus d'investigation dans Detective, consultez Utilisation d'Amazon Detective à des fins d'investigation dans le Guide de l'utilisateur Amazon Detective.

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 Detective.

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 vos résultats de sécurité provenant de plusieurs produits Services AWS (y compris Detective) et de AWS Partner Network (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.

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.

Amazon Security Lake

Amazon Security Lake est un service de lac de données de sécurité entièrement géré. Vous pouvez utiliser Security Lake pour centraliser automatiquement les données de sécurité provenant des AWS environnements, des fournisseurs SaaS, des sources sur site, des sources cloud et des sources tierces dans un lac de données spécialement conçu et stocké dans votre compte. AWS Security Lake vous aide à analyser les données de sécurité, afin que vous puissiez mieux comprendre votre posture de sécurité dans l'ensemble de votre organisation. Avec Security Lake, vous pouvez également améliorer la protection des charges de travail, des applications et des données.

Pour en savoir plus sur Security Lake, consultez le guide de l'utilisateur d'Amazon Security Lake. Pour en savoir plus sur l'utilisation conjointe de Detective et Security Lake, consultezDetective Integration avec Security Lake.

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

Concepts et terminologie d'Amazon Detective

Les termes et concepts suivants sont importants pour comprendre Amazon Detective et son fonctionnement.

Compte administrateur

Le Compte AWS qui possède un graphe de comportement et qui utilise le graphe de comportement à des fins d'investigation.

Le compte administrateur invite les comptes membres à apporter leurs données au graphe de comportement. Pour de plus amples informations, veuillez consulter the section called “Gestion des comptes membres”.

Pour le graphe du comportement de l'organisation, le compte administrateur est le compte administrateur Detective désigné par le compte de gestion de l'organisation. Pour plus d'informations, consultez the section called “Désignation du compte administrateur Detective”. Le compte administrateur Detective peut activer n'importe quel compte de l'organisation comme compte membre dans le graphe de comportement. Pour plus d'informations, consultez the section called “Gestion des comptes membres de l'organisation”.

Les comptes administrateurs peuvent également consulter l'utilisation des données pour le graphe de comportement et supprimer des comptes membres du graphe de comportement.

Organisation du système autonome (ASO)

L'organisation intitulée à laquelle un système autonome est attribué. Ce système autonome est un réseau hétérogène ou un ensemble de réseaux utilisant une logique et des politiques de routage similaires.

Graphe de comportement

Un ensemble lié de données généré à partir de données source entrantes associé à une ou plusieurs Comptes AWS.

Chaque graphe de comportement utilise la même structure de résultats, d'entités et de relations.

Compte d'administrateur délégué (AWS Organizations)

Dans Organizations, le compte administrateur délégué d'un service est capable de gérer l'utilisation d'un service pour l'organisation.

Dans Detective, le compte administrateur Detective est également le compte administrateur délégué, sauf si le compte administrateur Detective est le compte de gestion de l'organisation. Le compte de gestion de votre organisation ne peut pas être un administrateur délégué.

Dans Detective, l'autodélégation est autorisée. Un compte de gestion de l'organisation peut déléguer son propre compte pour être l'administrateur délégué de Detective, mais cela ne sera enregistré ou mémorisé que dans le cadre de Detective, et non dans le cadre des organisations.

Compte administrateur Detective

Le compte désigné par le compte de gestion de l'organisation comme étant le compte administrateur du graphe du comportement de l'organisation dans une région. Pour plus d'informations, consultez the section called "Désignation du compte administrateur Detective".

Detective recommande au compte de gestion de l'organisation de choisir un compte autre que le sien.

Si le compte n'est pas le compte de gestion de l'organisation, le compte administrateur Detective est également le compte administrateur délégué de Detective dans Organizations.

Données sources de Detective

Versions structurées et traitées des informations issues des types de flux suivants :

- Logs provenant de AWS des services, tels que AWS CloudTrail journaux et journaux Amazon VPC Flow
- GuardDuty résultats

Detective utilise les données sources de Detective pour remplir le graphe de comportement. Pour prendre en charge son analyse, Detective stocke également des copies de ses données sources.

Entité

Un élément extrait des données ingérées.

Chaque entité possède un type qui identifie le type d'objet qu'elle représente. Les exemples de types d'entités incluent les adresses IP, EC2 les instances Amazon et AWS utilisateurs.

Les entités peuvent être AWS les ressources que vous gérez ou les adresses IP externes qui ont interagi avec vos ressources.

Pour chaque entité, les données sources sont également utilisées pour renseigner les propriétés de l'entité. Les valeurs des propriétés peuvent être extraites directement des enregistrements sources, ou agrégées sur plusieurs enregistrements.

Résultat

Un problème de sécurité a été détecté par Amazon GuardDuty.

Groupe de résultats

Un ensemble de résultats, d'entités et de preuves connexes qui peuvent être liés au même événement ou au même problème de sécurité. Detective génère des groupes de résultats sur la base d'un modèle de machine learning intégré.

Preuve de Detective

Detective identifie des preuves supplémentaires liées à un groupe de résultats sur la base des données de votre graphe de comportement collectées au cours des 45 derniers jours. Ces preuves sont présentées sous la forme d'un résultat dont la valeur de gravité est Informationnelle. Les preuves fournissent des informations complémentaires qui mettent en évidence une activité inhabituelle ou un comportement inconnu potentiellement suspect au sein d'un groupe de résultats. Les géolocalisations récemment observées ou les API appels observés dans le cadre d'une découverte en sont un exemple. Pour le moment, ces résultats ne sont visibles que dans Detective et ne sont pas envoyés à Security Hub.

Vue d'ensemble des recherches

Une page unique qui fournit un résumé des informations relatives à un résultat.

Une vue d'ensemble des résultats contient la liste des entités impliquées dans les résultats. Dans la liste, vous pouvez passer au profil d'une entité.

Une vue d'ensemble des résultats contient également un volet de détails qui contient les attributs des résultats.

Entité à volume élevé

Entité qui est connectée à un grand nombre d'autres entités ou à partir d'un grand nombre d'autres entités pendant un intervalle de temps. Par exemple, une EC2 instance peut avoir des connexions provenant de millions d'adresses IP. Le nombre de connexions dépasse le seuil que Detective peut accepter.

Lorsque la durée de validité actuelle contient un intervalle de temps élevé, Detective en informe l'utilisateur.

Pour plus d'informations, consultez la section Affichage des informations sur les entités à volume élevé dans le Guide de l'utilisateur Amazon Detective.

Enquête

Processus qui consiste à trier les activités suspectes ou intéressantes, à déterminer leur validité, à identifier leur source ou cause sous-jacente, puis à déterminer la marche à suivre.

Compte membre

Un Compte AWS qu'un compte administrateur a invité à fournir des données à un graphe de comportement. Dans le graphe du comportement de l'organisation, un compte membre peut être un compte de l'organisation que le compte administrateur Detective a activé en tant que compte membre.

Les comptes membres invités peuvent répondre à l'invitation du graphe de comportement et supprimer leur compte du graphe de comportement. Pour plus d'informations, consultez the section called "Pour les comptes membres : gestion des invitations et des appartenances".

Les comptes de l'organisation ne peuvent pas modifier leur appartenance dans le graphe de comportement de l'organisation.

Tous les comptes membres peuvent également consulter les informations d'utilisation de leur compte sur les graphes de comportement auxquels ils fournissent des données.

Ils n'ont aucun autre accès au graphe de comportement.

Graphique du comportement de l'organisation

Le graphe de comportement appartenant au compte administrateur Detective. Le compte de gestion de l'organisation désigne le compte administrateur Detective. Pour plus d'informations, consultez the section called "Désignation du compte administrateur Detective".

Dans le graphe du comportement de l'organisation, le compte administrateur Detective contrôle si un compte de l'organisation est un compte membre. Un compte de l'organisation ne peut pas se supprimer lui-même du graphe de comportement de l'organisation.

Le compte administrateur Detective peut également inviter d'autres comptes à rejoindre le graphe de comportement de l'organisation.

Profil

Page unique qui fournit un ensemble de visualisations de données relatives à l'activité d'une entité.

En ce qui concerne les résultats, les profils aident les analystes à déterminer si le résultat est réellement préoccupant ou s'il s'agit d'un faux positif.

Les profils fournissent des informations pour appuyer une enquête dans un résultat, ou pour une recherche générale d'activités suspectes.

volet de profil

Une visualisation unique sur un profil. Chaque volet de profil est destiné à répondre à une ou plusieurs questions spécifiques afin d'aider un analyste dans le cadre d'une enquête.

Les volets de profil peuvent contenir des paires valeur-clé, des tableaux, des chronologies, des diagrammes à barres ou des diagrammes de géolocalisation.

Relation

Activité qui se produit entre des entités individuelles. Les relations sont également extraites des données sources entrantes.

Tout comme une entité, une relation possède un type qui identifie les types d'entités impliquées et le sens de la connexion. Un exemple de type de relation est une adresse IP se connectant à une EC2 instance Amazon.

Durée

La fenêtre temporelle utilisée pour définir les données affichées sur les profils.

La durée de validité par défaut d'un résultat correspond à la première et à la dernière fois que l'activité suspecte a été observée.

La durée de validité par défaut d'un profil d'entité correspond aux 24 heures précédentes.

Commencer à utiliser Amazon Detective

Ce didacticiel fournit une introduction à Amazon Detective. Vous allez apprendre comment activer Detective pour votre AWS compte. Vous apprendrez également comment vérifier que Detective a commencé à ingérer et à extraire les données de votre AWS compte dans votre graphe de comportement.

Lorsque vous activez Amazon Detective, Detective crée un graphe de comportement spécifique à une région dont votre compte est le compte administrateur. Il s'agit initialement du seul compte du graphe de comportement. Le compte administrateur peut ensuite inviter d'autres AWS comptes à apporter leurs données au graphique de comportement. Consultez Gestion des comptes.

En activant Detective dans une région pour la première fois, vous bénéficiez également d'un essai gratuit de 30 jours pour le graphe de comportement. Si le compte désactive Detective puis le réactive, aucun essai gratuit n'est disponible. Consultez the section called "À propos de la version d'essai gratuite des graphes de comportement".

Après l'essai gratuit, chaque compte figurant dans le graphe de comportement est facturé pour les données qu'il contient. Le compte administrateur peut suivre l'utilisation et voir le coût total prévu pour une période de 30 jours en général pour l'ensemble de son graphe de comportement. Pour plus d'informations, consultez the section called "Utilisation et coûts du compte administrateur". Les comptes membres peuvent suivre l'utilisation et le coût prévisionnel des graphes de comportement auxquels ils appartiennent. Pour de plus amples informations, veuillez consulter the section called "Suivi de l'utilisation du compte membre".

Rubriques

- Configuration de votre AWS compte
- Conditions préalables pour activer Detective
- Recommandations pour activer Detective
- Activation de Detective

Configuration de votre AWS compte

Avant d'activer Amazon Detective, vous devez disposer d'un Compte AWS. Si vous n'avez pas de AWS compte, procédez comme suit pour en créer un.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte en accédant à https://aws.amazon.com/et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu'utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

   Pour obtenir des instructions, consultez Création d'un ensemble d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

Conditions préalables pour activer Detective

Assurez-vous que les conditions suivantes sont remplies avant d'activer Detective.

Octroi des autorisations Detective requises

Avant de pouvoir activer Detective, vous devez vous assurer que votre principal d'IAM dispose des autorisations Detective requises. Le principal peut être un utilisateur ou un rôle existant que vous utilisez déjà, ou vous pouvez créer un nouvel utilisateur ou un nouveau rôle à utiliser pour Detective.

Lors de votre inscription aux services Amazon Web Services, (AWS), votre compte est automatiquement inscrit à tous les Services AWS, notamment à Amazon Detective. Toutefois, pour activer et utiliser Detective, vous devez d'abord configurer des autorisations qui vous permettent d'accéder à la console Amazon Detective et aux opérations d'API. Vous ou votre administrateur pouvez le faire en utilisant AWS Identity and Access Management (IAM) pour associer la politique `AmazonDetectiveFullAccess` gérée à votre principal IAM, ce qui donne accès à toutes les actions Detective. Sans ces autorisations IAM, vous pouvez consulter la page Get started with Detective dans la AWS console. Par conséquent, la console n'affichera aucun graphique actif tant que ces autorisations ne seront pas ajoutées, même si le service est activé.

AWS Command Line Interface Version prise en charge

Pour utiliser les tâches AWS CLI de Detective, la version minimale requise est 1.16.303.

Recommandations pour activer Detective

Pensez à suivre ces recommandations avant d'activer Detective

Alignement recommandé avec GuardDuty et AWS Security Hub

Si vous êtes inscrit à GuardDuty et AWS Security Hub, nous recommandons que votre compte soit un compte administrateur pour ces services. Si les comptes d'administrateur sont les mêmes pour les trois services, les points d'intégration suivants fonctionnent parfaitement.

- Dans GuardDuty notre Security Hub, lorsque vous consultez les détails d'une GuardDuty découverte, vous pouvez passer des détails de la recherche au profil de recherche du Detective.
- Dans Detective, lorsque vous étudiez une GuardDuty découverte, vous pouvez choisir l'option d'archiver cette découverte.

Si vous possédez différents comptes d'administrateur pour GuardDuty Security Hub, nous vous recommandons d'aligner les comptes d'administrateur en fonction du service que vous utilisez le plus fréquemment.

- Si vous l'utilisez GuardDuty plus fréquemment, activez Detective à l'aide du compte GuardDuty administrateur.

  Si vous utilisez AWS Organizations pour gérer des comptes, désignez le compte GuardDuty administrateur comme compte d'administrateur Detective pour l'organisation.
- Si vous utilisez Security Hub plus fréquemment, activez Detective à l'aide du compte administrateur du Security Hub.

  Si vous utilisez Organizations pour gérer des comptes, désignez le compte administrateur Security Hub comme compte administrateur Detective de l'organisation.

Si vous ne pouvez pas utiliser les mêmes comptes d'administrateur pour tous les services, vous pouvez éventuellement créer un rôle multicompte après avoir activé Detective. Ce rôle permet à un compte administrateur d'accéder à d'autres comptes.

Pour plus d'informations sur la manière dont IAM prend en charge ce type de rôle, consultez la section Fournir un accès à un utilisateur IAM sur un autre AWS compte que vous possédez dans le Guide de l'utilisateur IAM.

Mise à jour recommandée de la fréquence des GuardDuty CloudWatch notifications

Dans GuardDuty, les détecteurs sont configurés avec une fréquence de CloudWatch notification Amazon pour signaler les occurrences ultérieures d'une découverte. Cela inclut l'envoi de notifications à Detective.

Par défaut, la fréquence est de six heures. Cela signifie que même si un résultat se reproduit à de nombreuses reprises, les nouvelles occurrences n'apparaissent dans Detective que six heures plus tard.

Pour réduire le temps nécessaire à la réception de ces mises à jour par Detective, nous recommandons que le compte GuardDuty administrateur modifie le réglage de ses détecteurs à 15 minutes. Notez que la modification de la configuration n'a aucun effet sur le coût d'utilisation GuardDuty.

Pour plus d'informations sur la définition de la fréquence des notifications, consultez la section GuardDuty Monitoring Findings with Amazon CloudWatch Events dans le guide de GuardDuty l'utilisateur Amazon.

Activation de Detective

Vous pouvez activer Detective depuis la console Detective, l'API Detective ou l' AWS Command Line Interface.

Vous ne pouvez activer Detective qu'une seule fois dans chaque région. Si vous êtes déjà le compte administrateur d'un graphe de comportement dans la région, vous ne pouvez pas réactiver Detective dans cette région.

Console

Pour activer Detective (console)

1. Connectez-vous au AWS Management Console. Ouvrez ensuite la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Choisissez Démarrer.
3. Sur la page Activer Amazon Detective, Align administrator accounts (recommandé) explique la recommandation d'aligner les comptes administrateurs entre Detective et Amazon GuardDuty et AWS Security Hub. Consultez the section called "Alignement recommandé avec GuardDuty et AWS Security Hub".
4. Le bouton Attach IAM policy vous amène directement à la console IAM et ouvre la stratégie recommandée. Vous avez la possibilité d'associer la politique recommandée au principal que vous utilisez pour Detective. Si vous n'êtes pas autorisé à opérer dans la console IAM, dans la section Autorisations requises, vous pouvez copier la politique Amazon Resource Name (ARN) pour la fournir à votre administrateur IAM. Il peut ensuite associer la police en votre nom.

   Vérifiez que la politique IAM requise est en place.
5. La section Ajouter des balises vous permet d'ajouter des balises au graphe de comportement.

   Pour ajouter une balise, procédez comme suit :

   a. Sélectionnez Ajouter une nouvelle balise.

b. Pour Clé, entrez le nom de la balise.

c. Pour Valeur, saisissez la valeur de l'identification.

Pour supprimer une balise, choisissez l'option de Suppression pour cette balise.

6. Choisissez Activer Amazon Detective.
7. Après avoir activé Detective, vous pouvez inviter des comptes membres à accéder à votre graphe de comportement.

   Pour accéder à la page de Gestion du compte, choisissez Ajouter des membres maintenant. Pour plus d'informations sur l'invitation de comptes membres, consultez the section called "Gestion des comptes membres".

Detective API, AWS CLI

Vous pouvez activer Amazon Detective à partir de l'API Detective ou du AWS Command Line Interface.

Pour activer Detective (Detective API, AWS CLI)

- API Detective : utilisez l'opération `CreateGraph`.
- AWS CLI: À l'invite de commande, exécutez la commande `create-graph`.

```
aws detective create-graph --tags '{"tagName": "tagValue"}'
```

La commande suivante active Detective et définit la valeur de la balise `Department` sur`Security`.

```
aws detective create-graph --tags '{"Department": "Security"}'
```

Python script on GitHub

Vous pouvez activer Detective across Regions à l'aide du script Detective Python sur GitHub .Detective fournit un script open source GitHub qui effectue les opérations suivantes :

- Active Detective pour un compte administrateur dans une liste de régions spécifiée
- Ajoute une liste fournie de comptes membres à chacun des graphes de comportement obtenus

- Envoie des e-mails d'invitation aux comptes membres
- Accepte automatiquement les invitations pour les comptes membres.

Pour plus d'informations sur la configuration et l'utilisation GitHub des scripts, consultezthe section called "Scripts Python d'Amazon Detective".

Vérifier que Detective ingère les données de votre compte AWS

Une fois que vous avez activé Detective, celui-ci commence à ingérer et à extraire les données de votre AWS compte dans votre graphe de comportement.

Lors de l'extraction initiale, les données sont généralement disponibles dans le graphe de comportement dans les 2 heures.

Pour vérifier que Detective extrait des données, vous pouvez notamment rechercher des valeurs sur la page Detective Recherche.

Pour vérifier, par exemple, les valeurs sur la page de recherche

1. Ouvrez la console Amazon Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, sélectionnez Recherche.
3. Dans le menu Sélectionner un type, choisissez un type d'élément.

   Les exemples tirés de vos données contiennent un ensemble d'exemples d'identifiants du type sélectionné qui figurent dans les données de votre graphe de comportement.

   Si vous pouvez voir des exemples de valeurs, vous savez que les données sont ingérées et extraites dans votre graphe de comportement.

Données dans un graphe de comportement de Detective

Dans Amazon Detective, vous menez des enquêtes à l'aide des données d'un graphe de comportement de Detective. Dans cette section, vous découvrirez les principales sources de données utilisées dans un graphe de comportement de Detective et la manière dont Detective utilise les données sources pour le renseigner.

Un graphe de comportement est un ensemble de données liées générées à partir des données sources de Detective qui sont ingérées à partir d'un ou de plusieurs comptes Amazon Web Services (AWS).

Le graphe de comportement utilise les données source pour effectuer les opérations suivantes.

- Générer une vue d'ensemble de vos systèmes, utilisateurs et de leurs interactions au fil du temps
- Effectuer une analyse plus détaillée d'une activité spécifique pour vous aider à répondre aux questions qui se posent lorsque vous menez des enquêtes
- Corréler les ensembles de résultats, d'entités et de preuves susceptibles d'être liés au même événement ou au même problème de sécurité.

Notez que toutes les opérations d'extraction, de modélisation et d'analyse des données des graphes de comportement s'effectuent dans le contexte de chaque graphe de comportement individuel.

Chaque graphe de comportement contient les données d'un ou plusieurs comptes. Lorsqu'un compte active Detective, il devient le compte administrateur du graphe de comportement, et il choisit les comptes des membres pour le graphe de comportement. Un graphe de comportement peut comporter jusqu'à 1 200 comptes membres. Pour plus d'informations sur la façon dont un compte administrateur gère les comptes des membres dans un graphique de comportement, voir Gestion des comptes dans Detective.

Table des matières

- Comment Detective remplit un graphique de comportement
- Période de formation pour les nouveaux graphes comportementaux de Detective
- Vue d'ensemble de la structure de données du graphe de comportement
- Données source utilisées dans un graphe de comportement de Detective

Comment Detective remplit un graphique de comportement

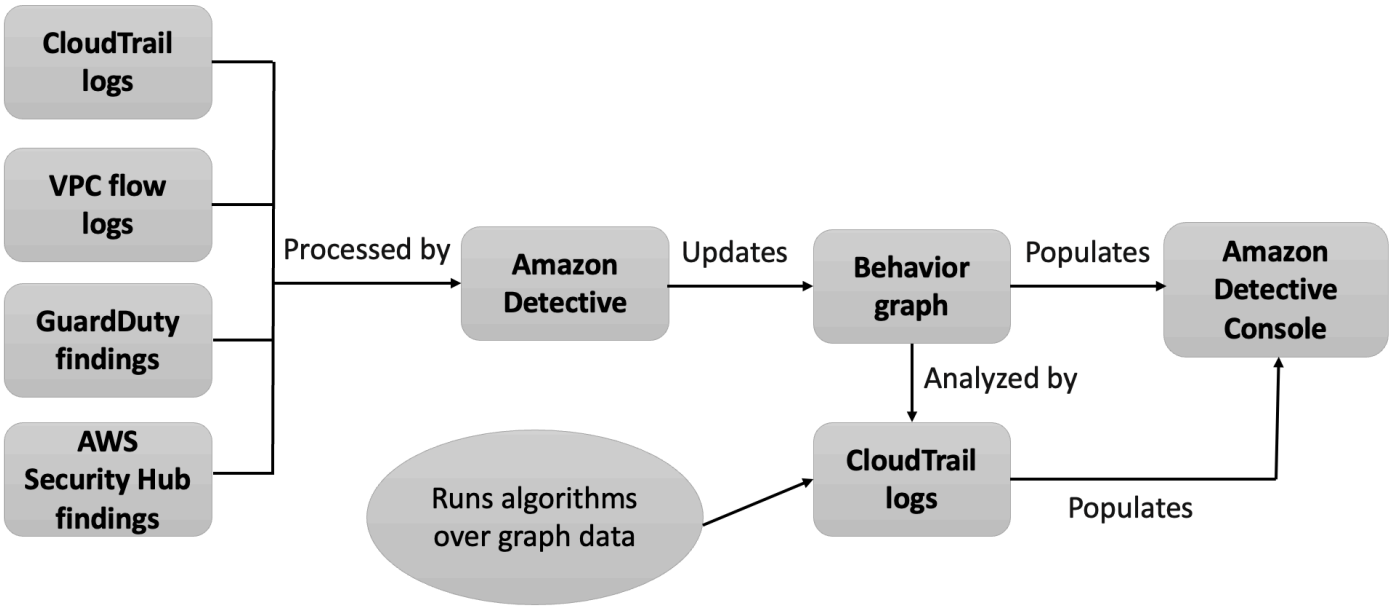
Pour fournir les données brutes nécessaires aux enquêtes, Detective rassemble des données provenant de l'ensemble de votre environnement AWS et au-delà, notamment les données suivantes :

- Données de journal, y compris Amazon Virtual Private Cloud (AmazonVPC) et AWS CloudTrail
- Conclusions d'Amazon GuardDuty
- Conclusions tirées de AWS Security Hub

Pour en savoir plus sur les données source utilisées dans un graphe de comportement, voir Données source utilisées dans un graphe de comportement.

Comment Detective traite les données sources

À mesure que de nouvelles données arrivent, Detective utilise une combinaison d'extraction et d'analyse pour renseigner le graphe de comportement.



Extraction de Detective

L'extraction est basée sur des règles de mappage configurées. Une règle de mappage indique essentiellement : « Chaque fois que vous voyez cette donnée, utilisez-la de cette manière spécifique pour mettre à jour les données du graphe de comportement ».

Par exemple, un enregistrement de données sources Detective entrant peut inclure une adresse IP. Si tel est le cas, Detective utilise les informations contenues dans cet enregistrement pour créer une nouvelle entité d'adresse IP ou mettre à jour une entité d'adresse IP existante.

Analyse Detective

Les analyses sont des algorithmes plus complexes qui analysent les données pour fournir un aperçu de l'activité associée aux entités.

Par exemple, un type d'analyse Detective analyse la fréquence de l'activité en exécutant des algorithmes. Pour les entités qui effectuent API des appels, l'algorithme recherche les API appels que l'entité n'utilise pas normalement. L'algorithme recherche également un pic important du nombre d'APIappels.

Les informations analytiques étayent les enquêtes en fournissant des réponses aux principales questions des analystes, et elles sont fréquemment utilisées pour remplir les volets de résultats et de profils des entités.

Période de formation pour les nouveaux graphes comportementaux de Detective

L'une des pistes d'investigation pour un résultat consiste à comparer l'activité pendant la durée de validité du résultat lié à l'activité qui s'est produite avant que le résultat ne soit détecté. Une activité qui n'a jamais été observée auparavant est peut-être plus susceptible d'être suspecte.

Certains volets de profil d'Amazon Detective mettent en évidence des activités qui n'ont pas été observées au cours de la période précédant le résultat. Plusieurs volets de profil affichent également une valeur de référence pour indiquer l'activité moyenne au cours des 45 jours précédant la durée de validité. Le périmètre temporel est le résumé de l'activité d'une entité au fil du temps.

Au fur et à mesure que de nouvelles données sont extraites vers votre graphe de comportement, Detective obtient une image plus précise des activités normales et inhabituelles au sein de votre organisation.

Cependant, pour créer cette image, Detective doit avoir accès à au moins deux semaines de données. La maturité de l’analyse Detective augmente également avec le nombre de comptes dans le graphe de comportement.

Les deux premières semaines suivant l’activation de Detective sont considérées comme une période de formation. Pendant cette période, les volets de profil qui comparent l’activité sur la durée de validité à celle des activités précédentes affichent un message indiquant que Detective est en période de formation.

Pendant la période d'essai, Detective vous recommande d'ajouter autant de comptes membres que possible au graphique de comportement. Detective dispose ainsi d’un plus grand pool de données, ce qui lui permet de générer une image plus précise de l’activité normale de votre organisation.

Vue d’ensemble de la structure de données du graphe de comportement

La structure de données du graphe de comportement définit la structure des données extraites et analysées. Elle définit également la manière dont les données sources sont mappées au graphe de comportement.

Types d’éléments dans la structure de données du graphe de comportement

La structure de données du graphe de comportement est constituée des éléments d’information suivants.

Entité

Une entité représente un élément extrait des données sources de Detective.

Chaque entité possède un type qui identifie le type d’objet qu’elle représente. Les exemples de types d'entités incluent les adresses IP, EC2 les instances Amazon et AWS les utilisateurs.

Pour chaque entité, les données sources sont également utilisées pour renseigner les propriétés de l’entité. Les valeurs des propriétés peuvent être extraites directement des enregistrements sources, ou agrégées sur plusieurs enregistrements.

Certaines propriétés se composent d’une valeur scalaire unique ou d’une valeur agrégée. Par exemple, pour une EC2 instance, Detective suit le type d'instance et le nombre total d'octets traités.

Les propriétés des séries chronologiques permettent de suivre l'activité au fil du temps. Par EC2 exemple, Detective suit au fil du temps les ports uniques qu'il a utilisés.

Relations

Une relation représente l'activité qui se produit entre des entités individuelles. Les relations sont également extraites des données sources Detective.

Tout comme une entité, une relation possède un type qui identifie les types d'entités impliquées et le sens de la connexion. Les adresses IP qui se connectent à des EC2 instances sont un exemple de type de relation.

Pour chaque relation individuelle, telle qu'une adresse IP spécifique se connectant à une instance spécifique, Detective suit les occurrences au fil du temps.

Types d'entités dans la structure de données du graphe de comportement

La structure de données du graphe de comportement comprend des types d'entités et de relations qui effectuent les opérations suivantes :

- Suivre les serveurs, les adresses IP et les agents utilisateurs utilisés
- Suivez les AWS utilisateurs, les rôles et les comptes utilisés
- Suivre les connexions réseau et les autorisations qui se produisent dans votre environnement AWS

La structure de données du graphe de comportement contient les types d'entités suivants.

AWS compte

AWS comptes présents dans les données source du Detective.

Pour chaque compte, Detective répond à plusieurs questions :

- Quels API appels le compte a-t-il utilisés ?
- Quels agents utilisateurs le compte a-t-il utilisés ?
- Quelles organisations du système autonome (ASOs) le compte a-t-il utilisées ?
- Dans quelles zones géographiques le compte a-t-il été actif ?

AWS rôle

AWS rôles présents dans les données source de Detective.

Pour chaque rôle, Detective répond à plusieurs questions :

- Quels API appels le rôle a-t-il utilisés ?
- Quels agents utilisateurs le rôle a-t-il utilisés ?
- Quel ASOs est le rôle utilisé ?
- Dans quelles zones géographiques le compte a-t-il été actif ?
- Quelles sont les ressources qui ont assumé ce rôle ?
- Quels rôles ce rôle a-t-il assumés ?
- Quelles sessions de rôle ont impliqué ce rôle ?

AWS utilisateur

AWS utilisateurs présents dans les données source de Detective.

Pour chaque utilisateur, Detective répond à plusieurs questions :

- Quels API appels l'utilisateur a-t-il utilisés ?
- Quels agents utilisateurs l'utilisateur a-t-il utilisés ?
- Dans quelles zones géographiques l'utilisateur a-t-il été actif ?
- Quels rôles cet utilisateur a-t-il assumés ?
- Quelles sessions de rôle ont impliqué cet utilisateur ?

Utilisateur fédéré

Instances d'un utilisateur fédéré. Voici quelques exemples d'utilisateurs fédérés :

- Une identité qui se connecte à l'aide du langage de balisage d'assertions de sécurité () SAML
- Une identité qui se connecte à l'aide de la fédération d'identité Web

Pour chaque utilisateur fédéré, Detective répond aux questions suivantes :

- Avec quel fournisseur d'identité l'utilisateur fédéré s'est-il authentifié ?
- Quel était le public de l'utilisateur fédéré ? L'audience identifie l'application qui a demandé le jeton d'identité Web de l'utilisateur fédéré.
- Dans quelles zones géographiques l'utilisateur fédéré a-t-il été actif ?
- Quels agents utilisateurs l'utilisateur fédéré a-t-il utilisés ?
- Qu'est-ce ASOs que l'utilisateur fédéré a utilisé ?
- Quels rôles cet utilisateur fédéré a-t-il assumés ?
- Quelles sessions de rôle ont impliqué cet utilisateur fédéré ?

EC2instance

EC2instances présentes dans les données source du Detective.

Par exempleEC2, Detective répond à plusieurs questions :

- Quelles adresses IP ont communiqué avec l'instance ?
- Quels ports ont été utilisés pour communiquer avec l'instance ?
- Quel volume de données a été envoyé vers et depuis l'instance ?
- Que VPC contient l'instance ?
- Quels API appels l'EC2instance a-t-elle utilisés ?
- Quels agents utilisateurs l'EC2instance a-t-elle utilisés ?
- Qu'est-ce que l'EC2instance ASOs a utilisé ?
- Dans quelles zones géographiques l'EC2instance a-t-elle été active ?
- Quels sont les rôles assumés EC2 par l'instance ?

Session de rôle

Instances d'une ressource qui assume un rôle. Chaque session de rôle est identifiée par un identifiant de rôle et un nom de session.

Pour chaque rôle, Detective répond à plusieurs questions :

- Quelles ressources ont été impliquées dans cette session de rôle ? En d'autres termes, quel rôle a été assumé et quelle ressource l'a assumé ?

  Notez que dans le cas d'une hypothèse de rôle inter-comptes, Detective ne peut pas identifier la ressource qui a assumé le rôle.
- Quels sont API les appels utilisés par la session de rôle ?
- Quels agents utilisateurs la session de rôle a-t-elle utilisés ?
- Qu'est-ce ASOs que la session de rôle a utilisée ?
- Dans quelles zones géographiques la session de rôle a-t-elle été active ?
- Quel utilisateur ou quel rôle a lancé cette session de rôle ?
- Quelles sessions de rôle ont débuté à partir de cette session de rôle ?

Résultat

Résultats découverts par Amazon GuardDuty qui sont intégrés aux données source du Detective.

Pour chaque résultat, Detective suit le type de résultat, l'origine et la fenêtre temporelle de l'activité du résultat.

Il stocke également des informations spécifiques au résultat, telles que les rôles ou les adresses IP impliqués dans l'activité détectée.

Adresse IP

Adresses IP présentes dans les données sources de Detective.

Pour chaque adresse IP, Detective répond à plusieurs questions :

- Quels API appels l'adresse a-t-elle utilisés ?
- Quels sont les ports utilisés par l'adresse ?
- Quels utilisateurs et agents utilisateurs ont utilisé l'adresse IP ?
- Dans quelles zones géographiques l'adresse IP a-t-elle été active ?
- À quelles EC2 instances cette adresse IP a-t-elle été attribuée et avec lesquelles elle a été communiquée ?

Compartiment S3

Compartiments S3 contenus dans les données sources de Detective.

Pour chaque compartiment S3, Detective répond aux questions suivantes :

- Quels principals ont interagi avec le compartiment S3 ?
- Quels API appels ont été effectués vers le compartiment S3 ?
- À partir de quels emplacements géographiques les directeurs ont-ils passé des API appels vers le compartiment S3 ?
- Quels agents utilisateurs ont été utilisés pour interagir avec le compartiment S3 ?
- Qu'est-ce qui a ASOs été utilisé pour interagir avec le compartiment S3 ?

Vous pouvez supprimer un compartiment S3, puis en créer un nouveau portant le même nom. Detective utilisant le nom du compartiment S3 pour identifier le compartiment S3, il les traite comme une entité de compartiment S3 unique. Sur le profil de l'entité, l'heure de création est la première heure de création. L'heure de suppression est l'heure de suppression la plus récente.

Pour afficher tous les événements de création et de suppression, définissez la durée de validité de manière à ce qu'elle commence par l'heure de création et se termine par l'heure de suppression. Dans le panneau Profil du volume global des API appels, affichez les détails

de l'activité pour la durée définie. Filtrez les API méthodes à afficher `Create` et `Delete` les méthodes. Consultez the section called “Volume global API d'appels”.

Agent utilisateur

Agents utilisateurs présents dans les données sources de Detective.

Pour chaque agent utilisateur, Detective répond à des questions telles que :

- Quels API appels l'agent utilisateur a-t-il utilisés ?
- Quels utilisateurs et quels rôles ont utilisé l'agent utilisateur ?
- Quelles adresses IP ont utilisé l'agent utilisateur ?

EKSCluster

EKSclusters présents dans les données source de Detective.

> **Note**
>
> Pour voir tous les détails de ce type d'entité, la source de données facultative des journaux d'EKSaudit doit être activée. Pour plus d'informations, voir Sources de données facultatives

Pour chaque EKS cluster, Detective répond à des questions telles que les suivantes :

- Quels API appels Kubernetes ont été exécutés dans ce cluster ?
- Quels utilisateurs et comptes de service Kubernetes (sujets) sont actifs dans ce cluster ?
- Quels conteneurs ont été lancés dans ce cluster ?
- Quelles images sont utilisées pour lancer des conteneurs dans ce cluster ?

Pod Kubernetes

Pods Kubernetes présents dans les données sources de Detective.

> **Note**
>
> Pour voir tous les détails de ce type d'entité, la source de données facultative des journaux d'EKSaudit doit être activée. Pour plus d'informations, voir Sources de données facultatives

Pour chaque pod, Detective répond à des questions telles que :

- Quelles images de conteneur présentes dans ce pod sont courantes dans mes comptes ?
- Quelle activité a été dirigée vers ce pod ?
- Quels sont les conteneurs utilisés dans ce pod ?
- Les registres provenant de conteneurs contenus dans ce pod sont-ils courants dans mes comptes ?
- Quels autres conteneurs s'exécutent dans les autres pods de la charge de travail ?
- Y a-t-il des conteneurs anormaux dans ce pod qui ne se trouvent pas dans les autres pods de la charge de travail ?

Image de conteneur

Images de conteneurs présentes dans les données sources de Detective.

> **Note**
>
> Pour voir tous les détails de ce type d'entité, la source de données facultative des journaux d'EKSaudit doit être activée. Pour plus d'informations, voir Sources de données facultatives

Pour chaque image de conteneur, Detective répond à des questions telles que :

- Quelles autres images de mon environnement partagent le même référentiel ou registre avec cette image ?
- Combien de copies de cette image sont exécutées dans mon environnement ?

Sujet Kubernetes

Sujets Kubernetes présents dans les données sources de Detective. Un sujet Kubernetes est un compte d'utilisateur ou de service.

> **Note**
>
> Pour voir tous les détails de ce type d'entité, la source de données facultative des journaux d'EKSaudit doit être activée. Pour plus d'informations, voir Sources de données facultatives

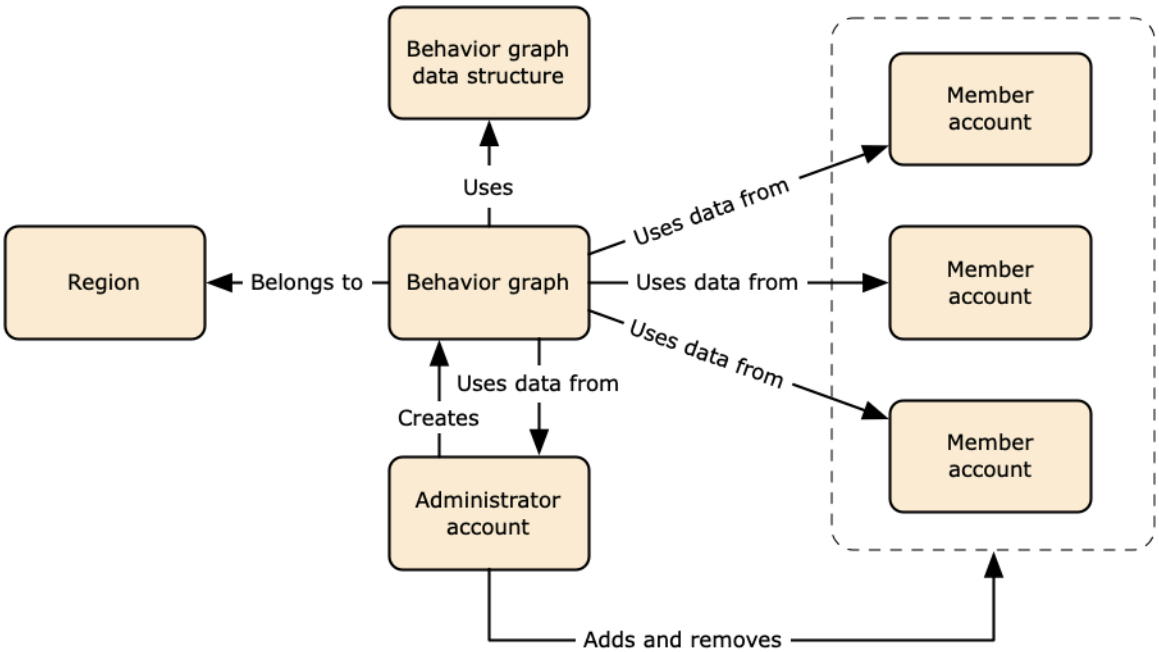
Pour chaque sujet, Detective répond à des questions telles que :

- Quels sont IAM les principaux responsables qui se sont authentifiés en tant que sujet ?
- Quels sont les résultats associés à ce sujet ?
- Quelles sont les adresses IP utilisées par le sujet ?

Données source utilisées dans un graphe de comportement de Detective

Pour remplir un graphe de comportement, Amazon Detective utilise les données source du compte administrateur du graphe de comportement et des comptes membres.

Avec Detective, vous pouvez accéder à un an de données historiques sur les événements. Ces données sont disponibles via un ensemble de visualisations qui montrent l'évolution du type et du volume d'activité au cours d'une période sélectionnée. Detective associe ces changements aux GuardDuty découvertes.



Pour plus de détails sur la structure de données du graphe de comportement, voir Présentation de la structure de données du graphe de comportement dans le Guide de l'utilisateur Detective.

Types de sources de données principales dans Detective

Detective ingère les données issues des types de AWS journaux suivants :

- AWS CloudTrail journaux
- Journaux de flux Amazon Virtual Private Cloud (AmazonVPC)
  - Ingère IPv4 et IPv6 enregistre à la fois, mais pas les MAC enregistrements produits par les adaptateurs Elastic Fabric.
  - Ingère les enregistrements du journal lorsque la valeur du `log-status` champ est en `OK` état. Pour plus d'informations, consultez les enregistrements du journal de flux dans le guide de VPC l'utilisateur Amazon.
  - Ingère les journaux de flux produits par les instances Amazon Elastic Compute Cloud exécutées VPCs uniquement dans ces instances. Aucune autre ressource, telle que les NAT passerelles, les RDS instances ou les clusters Fargate, n'est utilisée.
  - Ingère à la fois le trafic accepté et le trafic refusé.
- Pour les comptes enregistrés GuardDuty, Detective ingère également GuardDuty les résultats.

Detective consomme CloudTrail et VPC enregistre les événements à l'aide de flux et de journaux de flux indépendants CloudTrail et VPC dupliqués. Ces processus n'affectent ni n'utilisent vos configurations existantes CloudTrail et celles de vos journaux de VPC flux. Ils n'affectent pas non plus les performances de ces services et n'en augmentent pas les coûts.

Types de sources de données facultatives dans Detective

Detective propose des packages de sources optionnels en plus des trois sources de données proposées dans le package principal de Detective (le package de base inclut AWS CloudTrail les journaux, les journaux de VPC flux et GuardDuty les résultats). Un package de source de données facultatif peut être démarré ou arrêté à tout moment pour un graphe de comportement.

Detective propose un essai gratuit de 30 jours pour tous les packages sources principaux et facultatifs par région.

> **Note**
>
> Detective conserve toutes les données reçues de chaque package de source de données pendant un an maximum.

Les packages source facultatifs suivants sont actuellement disponibles :

- EKS journaux d'audit

Ce package de source de données facultatif permet à Detective d'ingérer des informations détaillées sur les EKS clusters de votre environnement et d'ajouter ces données à votre graphe de comportement. Detective met en corrélation les activités des utilisateurs avec les événements de AWS CloudTrail gestion et l'activité réseau avec Amazon VPC Flow Logs sans que vous ayez à activer ou à stocker ces journaux manuellement. Consultez Journaux EKS d'audit Amazon pour plus de détails.

- AWS constatations relatives à la sécurité

  Ce package de source de données facultatif permet à Detective d'ingérer des données depuis Security Hub et d'ajouter ces données à votre graphe de comportement. Consultez AWS constatations relatives à la sécurité pour plus de détails.

Démarrage ou arrêt d'une source de données facultative :

1. Ouvrez la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, sous Paramètres, choisissez Général.
3. Sous Packages source facultatifs, sélectionnez Mettre à jour. Sélectionnez ensuite la source de données que vous souhaitez activer ou désélectionner pour une source de données déjà activée et choisissez Mettre à jour pour modifier les packages de sources de données activés.

> **Note**
>
> Si vous arrêtez puis redémarrez une source de données facultative, vous constaterez une lacune dans les données affichées sur certains profils d'entité. Cet écart sera noté sur l'écran de la console et représente la période pendant laquelle la source de données a été arrêtée. Lorsqu'une source de données est redémarrée, Detective n'ingère pas de données rétroactivement.

Journaux EKS d'audit Amazon

Les journaux EKS d'audit Amazon sont un package de sources de données facultatif qui peut être ajouté à votre graphe de comportement Detective. Vous pouvez consulter les packages source facultatifs disponibles, ainsi que leur statut dans votre compte, depuis la page Paramètres de la console ou via le DetectiveAPI.

Un essai gratuit de 30 jours est fourni pour cette source de données. Pour en savoir plus, consultez Essai gratuit pour les sources de données facultatives.

L'activation des journaux EKS d'audit Amazon permet à Detective d'ajouter des informations détaillées sur les ressources créées avec Amazon EKS à votre graphe de comportement. Cette source de données améliore les informations fournies sur les types d'entités suivants : EKS Cluster, Kubernetes Pod, Container Image et Kubernetes subject.

En outre, si vous avez activé les journaux EKS d'audit en tant que source de données sur Amazon, GuardDuty vous pourrez consulter les informations relatives aux résultats de Kubernetes à partir de. GuardDuty Pour plus d'informations sur l'activation de cette source de données dans la GuardDuty section Protection de Kubernetes sur Amazon. GuardDuty

> **Note**
>
> Cette source de données est activée par défaut pour les nouveaux graphes de comportement créés après le 26 juillet 2022. Pour les graphes de comportement créés avant le 26 juillet 2022, ils doivent être activés manuellement.

Ajouter ou supprimer les journaux EKS d'audit Amazon en tant que source de données facultative :

1. Ouvrez la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, sous Paramètres, choisissez Général.
3. Sous Packages source, sélectionnez les journaux EKS d'audit pour activer cette source de données. S'il est déjà activé, sélectionnez-le à nouveau pour ne plus intégrer les journaux EKS d'audit dans votre graphe de comportement.

AWS constatations relatives à la sécurité

AWS security findings est un package de source de données facultatif qui peut être ajouté à votre graphe de comportement Detective.

Vous pouvez consulter les packages source facultatifs disponibles, ainsi que leur statut dans votre compte, depuis la page Paramètres de la console ou via le DetectiveAPI.

Un essai gratuit de 30 jours est fourni pour cette source de données. Pour en savoir plus, consultez Essai gratuit pour les sources de données facultatives.

L'activation des résultats de AWS sécurité permet à Detective d'utiliser les résultats de Security Hub agrégés par Security Hub à partir des services en amont dans un format de résultats standard appelé AWS Security Format (ASFF), qui élimine le besoin de longs efforts de conversion de données. Ensuite, il met en corrélation les résultats ingérées entre les différents produits afin de donner la priorité aux plus importants d'entre eux.

Ajouter ou supprimer des résultats AWS de sécurité en tant que source de données facultative :

> **Note**
>
> La source de données des résultats de AWS sécurité est activée par défaut pour les nouveaux graphes de comportement créés après le 16 mai 2023. Pour les graphes de comportement créés avant le 16 mai 2023, ils doivent être activés manuellement.

1. Ouvrez la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, sous Paramètres, choisissez Général.
3. Sous Packages source, sélectionnez les résultats AWS de sécurité pour activer cette source de données. S'il est déjà activé, sélectionnez-le à nouveau pour arrêter d'intégrer les résultats du AWS Security Finding Format (ASFF) dans votre graphe de comportement.

Résultats actuellement pris en charge

Detective ingère tous les ASFF résultats de Security Hub provenant de services détenus par Amazon ou AWS.

- Pour consulter la liste des intégrations de services prises en charge, consultez la section Intégrations de AWS services disponibles dans le guide de l' AWS Security Hub utilisateur.
- Pour la liste des ressources prises en charge, consultez la section Ressources du guide de l'utilisateur AWS Security Hub .
- AWS Les résultats de service dont le statut de conformité n'est pas défini sur `FAILED` et les résultats agrégés entre régions ne sont pas ingérés.

Comment Detective ingère et stocke les données sources

Lorsque Detective est activé, Detective commence à ingérer les données source depuis le compte administrateur du graphe de comportement. Au fur et à mesure que les comptes membres sont

ajoutés au graphe de comportement, Detective commence également à utiliser les données de ces comptes membres.

Les données source de Detective sont des versions structurées et traitées des flux d'origine. Pour faciliter l'analyse de Detective, Detective stocke des copies des données sources du Detective.

Le processus d'ingestion Detective alimente les compartiments Amazon Simple Storage Service (Amazon S3) dans le magasin de données source Detective. Lorsque de nouvelles données sources arrivent, d'autres composants de Detective les récupèrent et lancent les processus d'extraction et d'analyse. Pour plus d'informations, consultez la section Comment Detective utilise les données source pour remplir un graphe de comportement dans le Guide de l'utilisateur de Detective.

Comment Detective applique le quota de volume de données pour les graphes de comportement

Detective applique des quotas stricts quant au volume de données autorisé dans chaque graphe de comportement. Le volume de données est la quantité de données par jour qui est injectée dans le graphe de comportement du Detective.

Detective applique ces quotas lorsqu'un compte administrateur active Detective et lorsqu'un compte membre accepte une invitation à contribuer à un graphe de comportement.

- Si le volume de données d'un compte administrateur dépasse 10 To par jour, le compte administrateur ne peut pas activer Detective.
- Si le volume de données ajouté par un compte membre entraîne un dépassement du quota de 10 To par jour par le graphe de comportement, le compte membre ne peut pas être activé.

Le volume de données d'un graphe de comportement peut également augmenter naturellement au fil du temps. Detective vérifie chaque jour le volume de données du graphe de comportement pour s'assurer qu'il ne dépasse pas le quota.

Si le volume de données du graphe de comportement approche le quota, Detective affiche un message d'avertissement sur la console. Pour éviter de dépasser le quota, vous pouvez supprimer des comptes membres.

Si le volume de données du graphe de comportement dépasse 10 To par jour, vous ne pouvez pas ajouter de nouveau compte membre au graphe de comportement.

Si le volume de données du graphe de comportement dépasse 15 To par jour, Detective arrête d’ingérer les données dans le graphe de comportement. Les 15 To par jour reflètent à la fois le volume de données normal et les pics de volume de données. Lorsque ce quota est atteint, aucune nouvelle donnée n’est ingérée dans le graphe de comportement, mais les données existantes ne sont pas supprimées. Vous pouvez toujours utiliser ces données historiques à des fins d’investigation. La console affiche un message indiquant que l’ingestion de données est suspendue pour le graphe de comportement.

Si l'ingestion de données est suspendue, vous devez travailler avec vous Support pour la réactiver. Si possible, avant de contacter Support, essayez de supprimer les comptes des membres pour que le volume de données soit inférieur au quota. Cela facilite la réactivation de l’ingestion de données pour le graphe de comportement.

Utilisation du tableau de bord récapitulatif de Detective

Utilisez le tableau de bord récapitulatif d'Amazon Detective pour identifier les entités afin d'enquêter sur l'origine de l'activité au cours des dernières 24 heures. Le tableau de bord Amazon Detective Summary vous aide à identifier les entités associées à des types spécifiques d'activités inhabituelles. C'est l'un des nombreux points de départ possibles pour une enquête.

Pour afficher le tableau de bord Summary, dans le volet de navigation Detective, sélectionnez Summary. Le tableau de bord Summary s'affiche également par défaut lorsque vous ouvrez la console Detective pour la première fois.

Dans le tableau de bord récapitulatif, vous pouvez identifier les entités qui répondent aux critères suivants :

- Enquêtes révélant des événements de sécurité potentiels identifiés par Detective
- Entités impliquées dans une activité survenue dans des géolocalisations nouvellement observées
- Entités ayant effectué le plus grand nombre d'APIappels
- EC2instances ayant enregistré le plus grand volume de trafic
- Clusters de conteneurs contenant le plus grand nombre de conteneurs

Dans chaque panneau du tableau de bord récapitulatif, vous pouvez passer au profil de l'entité sélectionnée.

Lorsque vous consultez le tableau de bord récapitulatif, vous pouvez ajuster la durée du champ d'application pour afficher l'activité sur une période de 24 heures au cours des 365 jours précédents. Lorsque vous modifiez la date et l'heure de début, la date et l'heure de fin sont automatiquement mises à jour 24 heures après l'heure de début que vous avez choisie.

Avec Detective, vous pouvez accéder à un an de données historiques sur les événements. Ces données sont disponibles via un ensemble de visualisations qui montrent l'évolution du type et du volume d'activité au cours d'une période sélectionnée. Detective associe ces changements aux GuardDuty découvertes.

Pour plus d'informations sur les données source dans Detective, voir Données source utilisées dans un graphe de comportement.

Enquêtes

Le volet Enquêtes affiche les événements de sécurité potentiels identifiés par Detective. Dans le volet Investigations, vous pouvez consulter les enquêtes critiques ainsi que les rôles et utilisateurs AWS correspondants qui ont été affectés par des événements de sécurité au cours d’une période définie. Les enquêtes regroupent les indicateurs de compromission pour aider à déterminer si une AWS ressource est impliquée dans une activité inhabituelle susceptible d'indiquer un comportement malveillant et son impact.

Sélectionnez Afficher toutes les enquêtes pour consulter les résultats, trier les groupes de résultats et les détails des ressources afin d’accélérer votre enquête de sécurité. Les enquêtes sont affichées en fonction de la durée de validité sélectionnée. Vous pouvez ajuster a durée de validité pour visualiser les enquêtes sur une période de 24 heures au cours des 365 jours précédents. Vous pouvez passer directement à Investigations critiques pour consulter un rapport d’enquête détaillé.

Si vous identifiez un AWS rôle ou un utilisateur qui semble présenter une activité suspecte, vous pouvez passer directement du panneau Enquêtes au rôle ou à l'utilisateur pour poursuivre votre enquête. Passez à un rôle ou à un utilisateur et cliquez sur Exécuter une investigation pour générer un rapport d’investigation. Une fois que vous avez mené une enquête sur un rôle ou un utilisateur, le rôle ou l’utilisateur est déplacé vers l’onglet Enquêté.

Géolocalisations nouvellement observées

Les nouvelles géolocalisations observées mettent en évidence les emplacements géographiques qui étaient à l’origine de l’activité au cours des 24 heures précédentes, mais qui n’avaient pas été observés au cours de la période de référence précédente.

Le volet inclut jusqu’à 100 géolocalisations. Les emplacements sont indiqués sur la carte et répertoriés dans le tableau situé sous la carte.

Pour chaque géolocalisation, le tableau affiche le nombre d'APIappels échoués et réussis passés depuis cette géolocalisation au cours des 24 heures précédentes.

Vous pouvez étendre chaque géolocalisation pour afficher la liste des utilisateurs et des rôles ayant effectué des API appels depuis cette géolocalisation. Pour chaque principal, le tableau répertorie le type et les éléments associés Compte AWS.

Si vous identifiez un utilisateur ou un rôle qui vous semble suspect, vous pouvez passer directement du volet au profil de l'utilisateur ou du rôle pour poursuivre votre enquête. Pour passer à un profil, choisissez l'identifiant de l'utilisateur ou du rôle.

Detective détermine l'emplacement des demandes à l'aide des bases de MaxMind données GeoIP. MaxMind fait état d'une très grande précision de ses données au niveau des pays, bien que la précision varie en fonction de facteurs tels que le pays et le type de propriété intellectuelle. Pour plus d'informations MaxMind, consultez la section Géolocalisation MaxMind IP. Si vous pensez que l'une des données GeoIP est incorrecte, vous pouvez envoyer une demande de correction à Maxmind à l'adresse MaxMind Correct Geo Data. IP2

Groupes de résultats actifs au cours des 7 derniers jours

Les groupes de résultats actifs au cours des 7 derniers jours vous indiquent les regroupements corrélés de résultats de Detective, d'entités et de preuves survenues dans votre environnement au cours d'une période définie. Les regroupements mettent en corrélation une activité inhabituelle susceptible d'indiquer un comportement malveillant. Le tableau de bord récapitulatif affiche jusqu'à cinq groupes triés en fonction des groupes contenant les résultats les plus critiques actifs la semaine dernière.

Vous pouvez sélectionner des valeurs dans le contenu Tactique, Compte, Ressource et Résultats pour obtenir plus de détails.

Les groupes de résultats sont générés sur une base quotidienne. Si vous identifiez un groupe de résultats qui vous intéresse, vous pouvez sélectionner le titre pour accéder à une vue détaillée du profil du groupe afin de poursuivre votre recherche.

Rôles et utilisateurs ayant le plus grand volume API d'appels

Les rôles et utilisateurs ayant le plus grand volume d'APIappels identifient les utilisateurs et les rôles qui ont effectué le plus grand nombre d'APIappels au cours des dernières 24 heures.

Le volet peut inclure un maximum de 100 utilisateurs et rôles. Pour chaque utilisateur ou rôle, vous pouvez voir le type (utilisateur ou rôle) et le compte associé. Vous pouvez également voir le nombre d'APIappels émis par cet utilisateur ou ce rôle au cours des dernières 24 heures.

Par défaut, les rôles liés à un service sont affichés. Les rôles liés aux services peuvent générer de gros volumes d' AWS CloudTrail activité, ce qui déplace les principes que vous souhaitez

approfondir. Vous pouvez choisir de désactiver l'option Afficher les rôles liés à un service afin de filtrer les rôles liés à un service dans la vue récapitulative du tableau de bord.

Vous pouvez exporter un fichier de valeurs séparées par des virgules (.csv) contenant les données de ce panneau.

Il existe également une chronologie du volume d'APIappels pour les 7 derniers jours. La chronologie peut vous aider à déterminer si le volume d'APIappels est inhabituel pour ce principal.

Si vous identifiez un utilisateur ou un rôle pour lequel le volume d'APIappels semble suspect, vous pouvez passer directement du panneau au profil de l'utilisateur ou du rôle pour poursuivre votre enquête. Vous pouvez également consulter le profil du compte associé à l'utilisateur ou au rôle. Pour consulter un profil, choisissez l'utilisateur, le rôle ou l'identifiant du compte.

EC2instances avec le volume de trafic le plus élevé

EC2les instances présentant le volume de trafic le plus élevé identifient les EC2 instances ayant enregistré le volume total de trafic le plus important au cours des 24 heures précédentes.

Le panel peut inclure jusqu'à 100 EC2 instances. Pour chaque EC2 instance, vous pouvez voir le compte associé ainsi que le nombre d'octets entrants, d'octets sortants et le nombre total d'octets des 24 heures précédentes.

Vous pouvez exporter un fichier de valeurs séparées par une virgule (.csv) qui contient les données de ce volet.

Vous pouvez également consulter une chronologie indiquant le trafic entrant et sortant au cours des 7 jours précédents. La chronologie peut aider à déterminer si le volume de trafic est inhabituel dans ce EC2 cas.

Si vous identifiez une EC2 instance présentant un volume de trafic suspect, vous pouvez accéder directement du panneau au profil de l'EC2instance pour poursuivre votre enquête. Vous pouvez également consulter le profil du compte propriétaire de l'EC2instance. Pour consulter un profil, choisissez l'identifiant de l'EC2instance ou du compte.

Clusters de conteneurs avec le plus grand nombre de pods Kubernetes

Les clusters de conteneurs contenant le plus grand nombre de pods Kubernetes créés identifient les clusters ayant le plus grand nombre de conteneurs exécutés au cours des 24 heures précédentes.

Ce panel comprend jusqu'à 100 clusters organisés en fonction des clusters auxquels le plus de résultats sont associés. Pour chaque cluster, vous pouvez voir le compte associé, le nombre en cours de conteneurs dans le cluster et le nombre de résultats associés au cluster au cours des 24 heures précédentes. Vous pouvez exporter un fichier de valeurs séparées par une virgule (.csv) qui contient les données de ce volet.

Si vous identifiez un cluster présentant des résultats récents, vous pouvez passer directement du volet au profil du cluster et poursuivre votre enquête. Vous pouvez également passer au profil du compte propriétaire du cluster. Pour passer à un profil, choisissez le nom du cluster ou l'identifiant du compte.

Notification de valeur approximative

Pour les rôles et les utilisateurs ayant le plus grand volume d'APIappels et les EC2instances avec le plus grand volume de trafic, si une valeur est suivie d'un astérisque (*), cela signifie qu'il s'agit d'une approximation. La vraie valeur est égale ou supérieure à la valeur affichée.

La raison en est due à la méthode utilisée par Detective pour calculer le volume pour chaque intervalle de temps. Sur la page Résumé, l'intervalle de temps est d'une heure.

Pour chaque heure, Detective calcule le volume total pour les 1 000 utilisateurs, rôles ou EC2 instances ayant le plus grand volume. Il exclut les données relatives aux utilisateurs, rôles ou EC2 instances restants.

Si une ressource figure parfois parmi les 1 000 premières et parfois non, le volume calculé pour cette ressource peut ne pas inclure toutes les données. Les données relatives aux intervalles de temps où elle ne figure pas parmi les 1 000 premières sont exclues.

Notez que cela ne s'applique qu'à la page Résumé. Le profil de l'utilisateur, du rôle ou de l'EC2instance fournit des détails précis.

Comment Detective est utilisé pour les enquêtes

Amazon Detective vous permet d’analyser, d’enquêter et d’identifier rapidement la cause racine des résultats de sécurité ou des activités suspectes. Detective fournit des outils pour soutenir l'ensemble du processus d'enquête. Dans Detective, une enquête peut commencer à partir d’un résultat, d’un groupe de résultats ou d’une entité.

Phases d'investigation dans Detective

Tout processus d'enquête Detective comprend les phases suivantes :

Tri

Le processus d’enquête commence lorsque vous êtes informé d’une instance suspecte d’activité malveillante ou à haut risque. Par exemple, vous êtes chargé d'examiner les résultats ou les alertes découverts par des services tels qu'Amazon GuardDuty et Amazon Inspector.

Au cours de la phase de tri, vous déterminez si vous pensez que l’activité est vraiment positive (activité véritablement malveillante) ou s’il s’agit d’un faux positif (activité non malveillante ou à haut risque). Les profils de Detective prennent en charge le processus de tri en fournissant un aperçu de l’activité de l’entité concernée.

Pour les vrais positifs, passez à la phase suivante.

Champ d’application

Au cours de la phase de cadrage, les analystes déterminent l’étendue de l’activité malveillante ou à haut risque et la cause sous-jacente.

Le cadrage répond aux types de questions suivants :

- Quels systèmes et utilisateurs ont été compromis ?
- D’où vient l’attaque ?
- Depuis combien de temps dure l’attaque ?
- Y a-t-il une autre activité connexe à découvrir ? Par exemple, si un attaquant extrait des données de votre système, comment les a-t-il obtenues ?

Les visualisations Detective peuvent vous aider à identifier les autres entités impliquées ou affectées.

Réponse

La dernière étape consiste à répondre à l'attaque afin de l'arrêter, de minimiser les dégâts et d'empêcher qu'une attaque similaire ne se reproduise.

Points de départ d'une enquête Detective

Chaque enquête dans Detective a un point de départ essentiel. Par exemple, il se peut qu'on vous attribue un Amazon GuardDuty ou une AWS Security Hub découverte à examiner. Il se peut également que vous soyez préoccupé par une activité inhabituelle associée à une adresse IP spécifique.

Les points de départ habituels d'une enquête incluent les résultats détectés par les données sources de Detective GuardDuty et les entités extraites de ces données.

Résultats détectés par GuardDuty

GuardDuty utilise les données de votre journal pour détecter les cas suspects d'activités malveillantes ou à haut risque. Detective fournit des ressources qui vous aideront à étudier ces résultats.

Pour chaque résultat, Detective fournit les détails de résultat associés. Detective affiche également les entités, telles que les adresses IP et les AWS comptes, connectées à la découverte.

Vous pouvez ensuite explorer l'activité des entités impliquées afin de déterminer si l'activité détectée à partir du résultat constitue une véritable source de préoccupation.

Pour de plus amples informations, veuillez consulter the section called "Vue d'ensemble des résultats".

AWS résultats de sécurité agrégés par Security Hub

AWS Security Hub regroupe les résultats de sécurité provenant de différents fournisseurs de résultats en un seul endroit et vous fournit une vue complète de l'état de votre sécurité dans AWS. Security Hub élimine la complexité liée au traitement de grands volumes de résultats provenant de plusieurs fournisseurs. Cela réduit les efforts nécessaires pour gérer et améliorer la sécurité de tous vos AWS comptes, ressources et charges de travail. Detective fournit des ressources qui vous aideront à étudier ces résultats.

Pour chaque résultat, Detective fournit les détails de résultat associés. Detective affiche également les entités, telles que les adresses IP et les AWS comptes, connectées à la découverte.

Pour de plus amples informations, veuillez consulter the section called "Vue d'ensemble des résultats".

Entités extraites des données source de Detective

À partir des données source de Detective ingérées, Detective extrait des entités telles que les adresses IP et les utilisateurs AWS . Vous pouvez utiliser l'un d'entre eux comme point de départ d'une enquête.

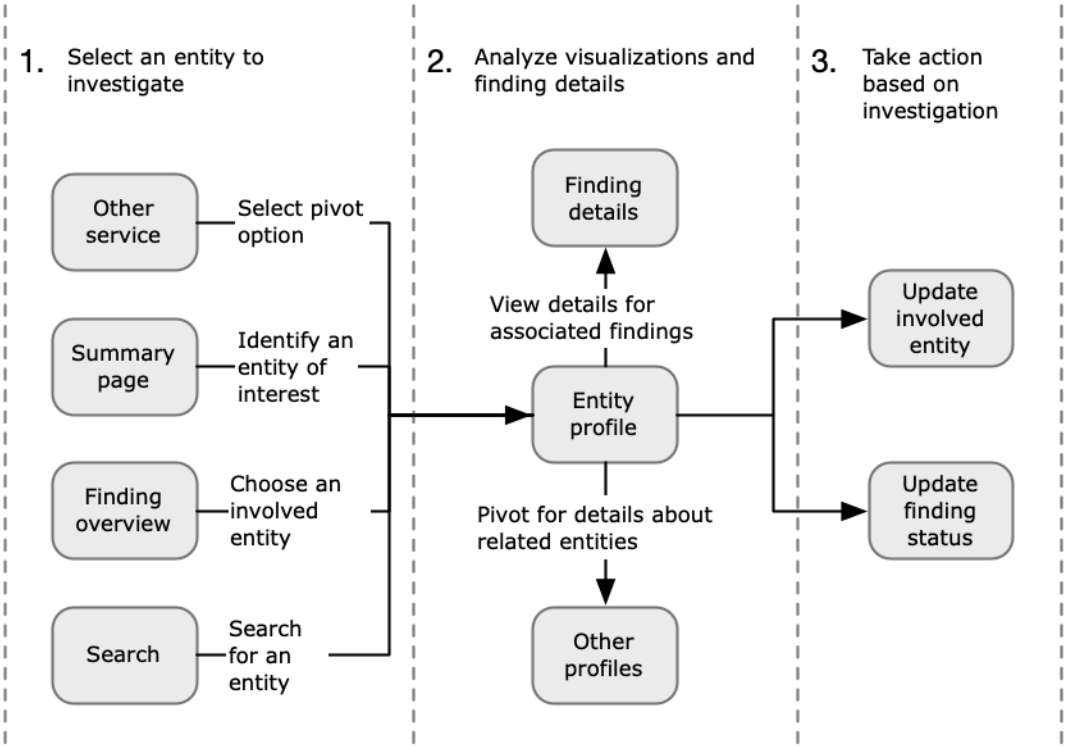
Detective fournit des informations générales sur l'entité, telles que l'adresse IP ou le nom d'utilisateur. Il fournit également des détails sur l'historique des activités. Par exemple, Detective peut signaler les autres adresses IP auxquelles une entité s'est connectée, a été connectée ou qu'elle a utilisées.

Pour de plus amples informations, veuillez consulter Analyse des entités.

Flux Detective Investigation

Vous pouvez utiliser Amazon Detective pour étudier une entité telle qu'une EC2 instance ou un AWS utilisateur. Vous pouvez également examiner les résultats de sécurité.

À un niveau élevé, l'image suivante montre le processus d'une Detective Investigation.



Étape 1 : sélectionnez l'entité à étudier

Lorsqu'ils examinent un résultat GuardDuty, les analystes peuvent choisir d'étudier une entité associée dans Detective. Consultez the section called "Pivotement depuis une autre console".

La sélection de l'entité vous amène au profil de l'entité dans Detective.

Étape 2 : analyser les visualisations sur les profils

Chaque profil d'entité contient un ensemble de visualisations générées à partir du graphe de comportement. Le graphe de comportement est créé à partir des fichiers journaux et d'autres données introduites dans Detective.

Les visualisations montrent l'activité liée à une entité. Vous utilisez ces visualisations pour répondre à des questions afin de déterminer si l'activité de l'entité est inhabituelle. Consultez Analyse des entités.

Pour vous aider à orienter l'enquête, vous pouvez utiliser le guide Detective fourni pour chaque visualisation. Le guide décrit les informations affichées, suggère des questions à poser et propose les prochaines étapes en fonction des réponses. Consultez the section called "Utilisation des instructions du volet de profil".

Chaque profil contient une liste de résultats associés. Vous pouvez consulter les détails d'un résultat ainsi que sa vue d'ensemble. Consultez the section called "Affichage des résultats d'une entité".

À partir d'un profil d'entité, vous pouvez passer à une autre entité et rechercher des profils de résultats, afin d'étudier plus en profondeur l'activité des actifs associés.

Étape 3 : passer à l'action

Sur la base des résultats de votre enquête, prenez les mesures appropriées.

En cas de résultat constituant un faux positif, vous pouvez archiver le résultat. Detective vous permet d'archiver GuardDuty les résultats. Pour plus de détails, consultez Archivage d'une GuardDuty recherche Amazon.

Dans le cas contraire, vous prenez les mesures appropriées pour remédier à la vulnérabilité et atténuer les dommages. Par exemple, vous devrez peut-être mettre à jour la configuration d'une ressource.

Detective Investigation

Vous pouvez utiliser Amazon Detective Investigation pour étudier IAM les utilisateurs et les IAM rôles à l'aide d'indicateurs de compromission, qui peuvent vous aider à déterminer si une ressource est impliquée dans un incident de sécurité. Un indicateur de compromission (IOC) est un artefact observé dans ou sur un réseau, un système ou un environnement qui peut (avec un niveau de confiance élevé) identifier une activité malveillante ou un incident de sécurité. Avec Detective Investigations, vous pouvez optimiser l'efficacité, vous concentrer sur les menaces de sécurité et renforcer les capacités de réponse aux incidents.

Detective Investigation utilise des modèles d'apprentissage automatique et des informations sur les menaces pour analyser automatiquement les ressources de votre AWS environnement afin d'identifier les incidents de sécurité potentiels. Cette fonctionnalité vous permet d'utiliser de manière proactive, efficace et effective l'automatisation basée sur le graphe de comportement de Detective pour améliorer les opérations de sécurité. Detective Investigation vous permet d'enquêter sur les tactiques d'attaque, les déplacements impossibles, les adresses IP signalées et la recherche de groupes. Il effectue les premières étapes de l'enquête de sécurité et génère un rapport mettant en évidence les risques identifiés par Detective, afin de vous aider à comprendre les événements de sécurité et à répondre aux incidents potentiels.

Rubriques

- Mener une enquête Detective
- Révision des rapports de Detective Investigations
- Comprendre un rapport de Detective Investigations
- Résumé du rapport Detective Investigations
- Téléchargement d'un rapport de Detective Investigations
- Archivage d'un rapport de Detective Investigations

Mener une enquête Detective

Utilisez Exécuter une investigation pour analyser les ressources telles que IAM les utilisateurs et IAM les rôles et pour générer un rapport d'enquête. Le rapport généré détaille les comportements anormaux qui indiquent une compromission potentielle.

Console

Suivez ces étapes pour exécuter une enquête Detective depuis la page Investigations à l'aide de la console Amazon Detective.

1. Connectez-vous à la console AWS de gestion. Ouvrez ensuite la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, choisissez Enquêtes.
3. Sur la page Enquêtes, choisissez Exécuter une investigation dans le coin supérieur droit.
4. Dans la section Sélectionner une ressource, vous pouvez effectuer une enquête de trois manières différentes. Vous pouvez choisir de lancer l'enquête pour une ressource recommandée par Detective. Vous pouvez exécuter l'enquête pour une ressource spécifique. Vous pouvez également enquêter sur une ressource depuis la page Rechercher de Detective.

   1. `Choose a recommended resource`— Detective recommande des ressources en fonction de son activité en matière de découvertes et de recherche de groupes. Pour exécuter l'enquête sur une ressource recommandée par Detective, dans le tableau des ressources recommandées, sélectionnez une ressource à examiner.

      Le tableau Ressources recommandées fournit les détails suivants :

      - Ressource ARN : nom de la ressource Amazon (ARN) de la AWS ressource.
      - Motif de l'enquête : affiche les principaux motifs menant à enquêter sur la ressource. Les motifs pour lesquels Detective recommande d'enquêter sur une ressource sont les suivants :
        - Si une ressource a été impliquée dans un résultat de haute gravité au cours des dernières 24 heures.
        - Si une ressource a été impliquée dans un groupe de résultats observé au cours des 7 derniers jours. Les groupes de résultats Detective vous permettent d'examiner plusieurs activités liées à un événement de sécurité potentiel. Pour en savoir plus, consultez the section called "Trouver des groupes".
        - Si une ressource a été impliquée dans un résultat observé au cours des 7 derniers jours.
      - Dernier résultat : les résultats les plus récents sont placés en tête de liste.
      - Type de ressource : identifie le type de ressource. Par exemple, un AWS utilisateur ou un AWS rôle.

2. `Specify an AWS role or user with an ARN`— Vous pouvez sélectionner un AWS rôle ou un AWS utilisateur et lancer une enquête pour la ressource en question.

   Suivez ces étapes pour étudier un type de ressource spécifique.

   a. Dans la liste déroulante Sélectionner le type de ressource, sélectionnez AWS un rôle ou un AWS utilisateur.

   b. Entrez la ressource ARN de la IAM ressource. Pour plus de détails sur ResourceARNs, consultez Amazon Resource Names (ARNs) dans le guide de IAM l'utilisateur.

3. `Find a resource to investigate from the Search page`— Vous pouvez effectuer des recherches dans toutes vos IAM ressources depuis la page Detective Search.

   Procédez comme suit pour rechercher une ressource à partir de la page de recherche.

   a. Dans le volet de navigation, sélectionnez Recherche.

   b. Dans la page de recherche, recherchez une IAM ressource.

   c. Accédez à la page de profil de la ressource et lancez une enquête à partir de là.

5. Dans la section Durée de l'enquête, choisissez la durée de l'enquête afin d'évaluer l'activité de la ressource sélectionnée. Vous pouvez sélectionner une date de début et une heure de début, ainsi qu'une date de fin et une heure de fin au UTC format. La fenêtre de durée de validité sélectionnée peut être comprise entre un minimum de 3 heures et un maximum de 30 jours.
6. Choisissez Exécuter une enquête.

API

Pour exécuter une enquête par programmation, utilisez le StartInvestigationDetective. API Pour exécuter une enquête à l'aide de la AWS Command Line Interface (AWS CLI), exécutez la commande start-investigation.

Dans votre demande, utilisez les paramètres suivants pour effectuer une enquête dans Detective :

- `GraphArn`— Spécifiez le nom de ressource Amazon (ARN) du graphe de comportement.
- `EntityArn`— Spécifiez le nom de ressource Amazon unique (ARN) de l'IAMutilisateur et du IAM rôle.

- `ScopeStartTime` : spécifiez éventuellement la date et l'heure à partir desquelles l'enquête doit commencer. La valeur est une chaîne au format UTC ISO86 01. Par exemple, `2021-08-18T16:35:56.284Z`.
- `ScopeEndTime` : spécifiez éventuellement la date et l'heure auxquelles l'enquête doit se terminer. La valeur est une chaîne au format UTC ISO86 01. Par exemple, `2021-08-18T16:35:56.284Z`.

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 detective start-investigation \
--graph-arn arn:aws:detective:us-
east-1:123456789123:graph:fdac8011456e4e6182facb26dfceade0
 --entity-arn arn:aws:iam::123456789123:role/rolename --scope-start-
time 2023-09-27T20:00:00.00Z
--scope-end-time 2023-09-28T22:00:00.00Z
```

Vous pouvez également exécuter une enquête à partir des pages suivantes de Detective :

- Une page de profil IAM d'utilisateur ou de IAM rôle dans Detective.
- Volet de visualisation de graphique d'un groupe de résultats.
- Colonne Actions d'une ressource impliquée.
- IAMutilisateur ou IAM rôle sur une page de recherche.

Une fois que Detective a effectué l'enquête pour une ressource, un rapport d'enquête est généré. Pour accéder au rapport, accédez à Investigations dans le volet de navigation.

Révision des rapports de Detective Investigations

Les rapports d'enquêtes vous permettent de consulter les rapports générés pour les enquêtes que vous avez menées précédemment dans Detective.

Pour examiner les rapports d'enquête

1. Connectez-vous à la console AWS de gestion. Ouvrez ensuite la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, choisissez Enquêtes.

Notez les attributs suivants d'un rapport d'enquête.

- ID : identifiant généré pour le rapport d'enquête. Vous pouvez choisir cet identifiant pour lire un résumé du rapport d'enquête, qui contient les détails de l'enquête.
- Statut : chaque enquête est associée à un statut basé sur l'état d'achèvement de l'enquête. Les valeurs d'état peuvent être En cours, Réussi ou Échoué.
- Niveau de gravité : un niveau de gravité est attribué à chaque enquête. Detective attribue automatiquement un niveau de gravité au résultat.

  Un niveau de gravité représente la disposition telle qu'analysée par l'étude d'une seule ressource pour une durée de validité donnée. Un niveau de gravité signalé par une enquête n'implique ni n'indique le caractère critique ou l'importance que pourrait avoir une ressource affectée pour votre organisation.

  Les valeurs de gravité de l'enquête peuvent être critiques, élevées, moyennes, faibles ou indicatives, en allant du niveau le plus grave au moins sévère.

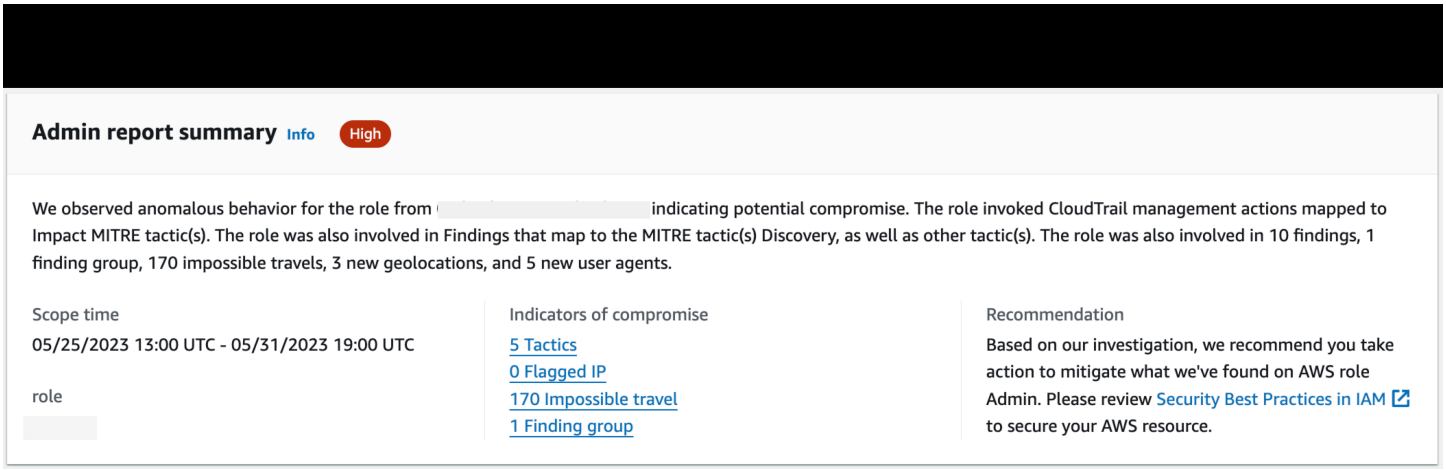
  Les enquêtes auxquelles est attribuée une valeur de gravité critique ou élevée doivent être prioritaires pour une inspection plus approfondie, car elles sont plus susceptibles de représenter des problèmes de sécurité à fort impact identifiés par Detective.
- Entité : la colonne Entité contient des détails sur les entités spécifiques détectées au cours de l'enquête. Certaines entités sont des AWS comptes, telles que l'utilisateur et le rôle.
- Statut : la colonne Date de création contient des détails sur la date et l'heure auxquelles le rapport d'enquête a été créé pour la première fois.

Comprendre un rapport de Detective Investigations

Un rapport de Detective Investigations fournit un résumé des comportements inhabituels ou des activités malveillantes indiquant une compromission. Il répertorie également les recommandations suggérées par Detective pour atténuer les risques de sécurité.

Pour consulter un rapport d'enquête pour un identifiant d'enquête spécifique.

1. Connectez-vous à la console AWS de gestion. Ouvrez ensuite la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, choisissez Enquêtes.
3. Dans le tableau Rapports, sélectionnez un identifiant d'enquête.



Detective génère le rapport pour la durée de validité et l'utilisateur sélectionnés. Le rapport contient une section sur les indicateurs de compromission qui inclut des détails concernant un ou plusieurs des indicateurs de compromission énumérés ci-dessous. Au fur et à mesure que vous passez en revue chaque indicateur de compromis, choisissez éventuellement un élément à explorer et à examiner en détail.

- Tactiques. Techniques et procédures — Identifie les tactiques, techniques et procédures (TTPs) utilisées lors d'un événement de sécurité potentiel. Le framework MITRE ATT &CK est utilisé pour comprendre leTTPs. Les tactiques sont basées sur la matrice MITRE ATT &CK pour Enterprise.
- Adresses IP signalées par le Threat Intelligence : les adresses IP suspectes sont signalées et identifiées comme des menaces critiques ou graves sur la base des informations du Detective Threat Intelligence.
- Déplacement impossible : détecte et identifie les activités inhabituelles et impossibles des utilisateurs associées à un compte. Par exemple, cet indicateur répertorie un changement radical entre l'emplacement source et l'emplacement de destination d'un utilisateur dans un court laps de temps.
- Groupe de résultats associé : affiche plusieurs activités liées à un événement de sécurité potentiel. Detective utilise des techniques d'analyse de graphes qui déduisent les relations entre les résultats et les entités, puis les regroupe en un groupe de résultat.
- Résultats connexes : activités connexes associées à un événement de sécurité potentiel. Répertorie toutes les catégories distinctes de preuves liées à la ressource ou au groupe de résultats.
- Nouvelles géolocalisations : identifie les nouvelles géolocalisations utilisées au niveau de la ressource ou du compte. Par exemple, cet indicateur répertorie une géolocalisation observée qui est une localisation peu fréquente ou inutilisée en fonction de l'activité précédente de l'utilisateur.

- Nouveaux agents utilisateurs : identifie les nouveaux agents utilisateurs utilisés au niveau de la ressource ou du compte.
- Nouveau ASOs — Identifie les nouvelles Organisations de systèmes autonomes (ASOs) utilisées au niveau des ressources ou des comptes. Par exemple, cet indicateur répertorie une nouvelle organisation affectée en tant queASO.

Résumé du rapport Detective Investigations

Le résumé des enquêtes met en évidence les indicateurs anormaux qui nécessitent une attention particulière pour la durée de validité sélectionnée. À l'aide du résumé, vous pouvez identifier plus rapidement la cause première des problèmes de sécurité potentiels, identifier les modèles et comprendre les ressources affectées par les événements de sécurité.

Dans le résumé du rapport d'enquête détaillé, vous pouvez afficher les détails suivants.

Vue d'ensemble des enquêtes

Dans le panneau Vue d'ensemble, vous pouvez voir une visualisation IPs des activités très graves, qui peut donner plus de contexte sur le parcours d'un attaquant.

Detective met en évidence une activité inhabituelle au cours de l'enquête, par exemple l'impossibilité pour l'IAMutilisateur de se rendre d'une source à une destination lointaine.

Detective associe les enquêtes aux tactiques, techniques et procédures (TTPs) utilisées lors d'un éventuel événement de sécurité. Le framework MITRE ATT &CK est utilisé pour comprendre leTTPs. Les tactiques sont basées sur la matrice MITRE ATT &CK pour Enterprise.

Indicateurs d'enquêtes

Vous pouvez utiliser les informations du volet Indicateurs pour déterminer si une ressource AWS est impliquée dans une activité inhabituelle susceptible d'indiquer un comportement malveillant et son impact. Un indicateur de compromission (IOC) est un artefact observé dans ou sur un réseau, un système ou un environnement qui peut (avec un niveau de confiance élevé) identifier une activité malveillante ou un incident de sécurité.

Téléchargement d'un rapport de Detective Investigations

Vous pouvez télécharger le rapport Detective Investigations au JSON format, pour l'analyser plus en profondeur ou le stocker dans votre solution de stockage préférée, telle qu'un compartiment Amazon S3.

Pour télécharger un rapport d'enquête à partir du tableau Rapports.

1. Connectez-vous à la console AWS de gestion. Ouvrez ensuite la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, choisissez Enquêtes.
3. Sélectionnez une enquête dans le tableau Rapports, puis choisissez Télécharger.

Pour télécharger un rapport d'enquête à partir de la page de synthèse.

1. Connectez-vous à la console AWS de gestion. Ouvrez ensuite la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, choisissez Enquêtes.
3. Sélectionnez une enquête dans le tableau Rapports.
4. Sur la page récapitulative des enquêtes, choisissez Télécharger.

Archivage d'un rapport de Detective Investigations

Lorsque vous avez terminé votre enquête dans Amazon Detective, vous pouvez archiver le rapport d'enquête. Une enquête archivée indique que vous avez terminé de l'examiner.

Vous pouvez archiver ou désarchiver une enquête uniquement si vous avez la qualification Detective Administrator. Detective conserve vos enquêtes archivées pendant 90 jours.

Pour archiver un rapport d'investigation à partir du tableau Rapports.

1. Connectez-vous à la console AWS de gestion. Ouvrez ensuite la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, choisissez Enquêtes.
3. Sélectionnez une enquête dans le tableau Rapports, puis choisissez Archive.

Pour archiver un rapport d'enquête à partir de la page de résumé.

1. Connectez-vous à la console AWS de gestion. Ouvrez ensuite la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, choisissez Enquêtes.
3. Sélectionnez une enquête dans le tableau Rapports.

4. Sur la page récapitulative des enquêtes, choisissez Archive.

Analyse des résultats dans Amazon Detective

Un résultat est un cas d'activité potentiellement malveillante ou d'un autre risque qui a été détecté. Amazon GuardDuty et les résultats AWS de sécurité sont chargés dans Amazon Detective afin que vous puissiez utiliser Detective pour enquêter sur l'activité associée aux entités impliquées. GuardDuty les résultats font partie du package principal de Detective et sont ingérés par défaut. Tous les autres résultats AWS de sécurité agrégés par Security Hub sont ingérés en tant que source de données facultative. Voir Données source utilisées dans un graphe de comportement pour plus de détails.

Une vue d'ensemble d'un résultat de Detective fournit des informations détaillées sur le résultat. Elle affiche également un résumé des entités impliquées, avec des liens vers les profils d'entités associés.

Si un résultat est corrélé à une activité plus importante, Detective vous invite désormais à accéder à ce groupe de résultats. Nous vous recommandons d'utiliser des groupes de résultats pour poursuivre votre enquête, car les groupes de résultats vous permettent d'examiner plusieurs activités liées à un événement de sécurité potentiel. Consultez the section called "Trouver des groupes".

Amazon Detective fournit une visualisation interactive des groupes de résultats. Cette visualisation est conçue pour vous aider à étudier les problèmes plus rapidement et de manière plus approfondie avec moins d'efforts. Le volet de visualisation de groupe de résultats affiche les résultats et les entités impliquées dans un groupe de résultats. Vous pouvez utiliser cette visualisation interactive pour analyser, comprendre et trier l'impact du groupe de résultats. Ce volet permet de visualiser les informations présentées dans le tableau Entités impliquées et résultats impliqués. Dans la présentation visuelle, vous pouvez sélectionner des résultats ou des entités pour une analyse plus approfondie. Consultez la section Recherche d'une visualisation de groupe.

Table des matières

- Analyse d'une vue d'ensemble des résultats dans Detective
- Analyse des groupes de résultats
- Récapitulatif des groupes de résultats optimisé par l'IA générative
- Archivage d'une recherche sur Amazon GuardDuty

Analyse d'une vue d'ensemble des résultats dans Detective

Une vue d'ensemble d'un résultat de Detective fournit des informations détaillées sur le résultat. Elle affiche également un résumé des entités impliquées, avec des liens vers les profils d'entités associés.

Durée de validité prise en compte pour la vue d'ensemble des résultats

La durée de validité d'une vue d'ensemble des résultats est définie en fonction de la fenêtre temporelle de résultats. La fenêtre temporelle de résultats fait apparaître la première et la dernière fois que l'activité de résultat a été observée.

Détails d'un résultat

Le volet de droite contient les détails du résultat. Il s'agit des informations fournies par le fournisseur de résultats.

À partir des détails du résultat, vous pouvez également archiver le résultat. Pour plus de détails, consultez Archivage d'une GuardDuty recherche Amazon.

Entités associées

La vue d'ensemble des résultats contient une liste des entités impliquées dans le résultat. Pour chaque entité, la liste fournit des informations générales sur l'entité. Ces informations reflètent les informations figurant dans le volet de profil des détails de l'entité sur le profil d'entité correspondant.

Vous pouvez appliquer un filtre à la liste en utilisant un type d'entité. Vous pouvez également filtrer la liste en fonction du texte de l'identificateur d'entité.

Pour passer au profil d'une entité, choisissez Voir le profil. Lorsque vous passez au profil d'entité, les événements suivants se produisent :

- La durée de validité est définie sur la fenêtre temporelle de résultats.
- Dans le volet Résultats associés de l'entité, le résultat est sélectionné. Les détails des résultats restent affichés à droite du profil de l'entité.

Résolution des problèmes liés au message « Page introuvable »

Lorsque vous accédez à une entité ou à un résultat dans Detective, le message d'erreur Page introuvable peut s'afficher.

Pour résoudre ce problème, procédez de l'une des manières suivantes :

- Assurez-vous que l'entité ou le résultat appartient à l'un de vos comptes membres. Pour plus d'informations sur la façon de consulter les comptes des membres, consultez la section Affichage de la liste des comptes.
- Assurez-vous que votre compte administrateur est aligné sur Security Hub GuardDuty et/ou qu'il est compatible avec Security Hub pour passer de ces services à Detective. Pour les recommandations, consultez la section Alignement recommandé avec Security Hub GuardDuty et Security Hub.
- Vérifiez que le résultat a été trouvé une fois que le compte membre a accepté votre invitation.
- Vérifiez que le graphique de comportement Detective ingère des données provenant d'un paquetage de source de données facultatif. Pour plus d'informations sur les données source utilisées dans les graphes de comportement de Detective, voir Données source utilisées dans un graphe de comportement.

- Pour permettre à Detective d'ingérer des données depuis Security Hub et de les ajouter à votre graphe de comportement, vous devez activer Detective for AWS security findings en tant que package de source de données. Pour plus d'informations, consultez les résultats AWS de sécurité.

- Si vous naviguez vers le profil d'une entité ou que vous trouvez une vue d'ensemble dans Detective, assurez-vous que le format URL est correct. Pour plus de détails sur la création d'un profilURL, voir Naviguer vers le profil d'une entité ou rechercher une vue d'ensemble à l'aide URL de.

Analyse des groupes de résultats

Les groupes de résultats Amazon Detective vous permettent d'examiner plusieurs activités liées à un événement de sécurité potentiel. Un groupe de recherche dans Amazon Detective est créé lorsque Detective détecte un schéma ou une relation entre plusieurs résultats qui suggèrent qu'ils sont liés au même incident de sécurité potentiel. Ce regroupement permet de gérer et d'étudier les résultats connexes de manière plus efficace.

Vous pouvez analyser la cause première des GuardDuty résultats très graves à l'aide de groupes de recherche. Si un auteur de menaces tente de compromettre votre AWS environnement, il exécute généralement une séquence d'actions qui aboutit à de multiples constatations de sécurité et à des comportements inhabituels. Ces actions sont souvent réparties dans le temps et dans des entités.

Lorsque les résultats de sécurité sont étudiés isolément, cela peut mener à une interprétation erronée de leur importance et à la difficulté d'en trouver la cause première. Amazon Detective résout ce problème en appliquant une technique d'analyse graphique qui déduit les relations entre les résultats et les entités, puis les regroupe. Nous recommandons de considérer les groupes de résultats comme point de départ pour étudier les entités impliquées et les résultats.

Detective analyse les données issues des résultats et les regroupe avec d'autres résultats susceptibles d'être liés en fonction des ressources qu'ils partagent. Par exemple, les résultats liés à des actions entreprises par des sessions ayant le même IAM rôle ou provenant de la même adresse IP sont très susceptibles de faire partie de la même activité sous-jacente. Il est utile d'étudier les résultats et les preuves en tant que groupe, même si les associations établies par Detective ne sont pas liées.

Les groupes de recherche sont créés en fonction des critères suivants.

- Proximité temporelle — Les constatations survenues dans un laps de temps rapproché sont souvent regroupées, car elles sont probablement liées au même incident.
- Entités communes : les résultats impliquant les mêmes entités, telles que les adresses IP, les utilisateurs ou les ressources, sont regroupés. Cela permet de comprendre l'ampleur de l'incident dans les différentes parties de l'environnement.
- Modèles et comportements — Detective analyse les modèles et les comportements contenus dans les résultats, tels que des types d'attaques similaires ou des activités suspectes, afin de déterminer les relations et de les regrouper en conséquence.
- Tactiques, techniques et procédures (TTPs) — Les résultats présentant des similitudesTTPs, tels que décrits dans des cadres tels que MITRE ATT &CK, sont regroupés pour mettre en évidence les attaques coordonnées potentielles.

Ces critères permettent de rationaliser le processus d'enquête afin que vous puissiez vous concentrer sur les résultats corrélés qui représentent probablement le même incident de sécurité.

Outre les résultats, chaque groupe comprend les entités impliquées dans les résultats. Les entités peuvent inclure des ressources extérieures, AWS telles que des adresses IP ou des agents utilisateurs.

> **Note**
>
> Une fois qu'une première GuardDuty constatation liée à une autre constatation a été effectuée, le groupe de recherche contenant toutes les constatations connexes et toutes les entités impliquées est créé dans les 48 heures.

Comprendre la page de groupes de résultats

La page des groupes de recherche répertorie tous les groupes de recherche collectés par Amazon Detective à partir de votre graphe de comportement. Prenez note des attributs suivants relatifs à la recherche de groupes :

Niveau de gravité d'un groupe

Une gravité est attribuée à chaque groupe de constatations en fonction AWS de la gravité du Security Finding Format (ASFF) des résultats associés. ASFFconstatant que les valeurs de gravité sont critiques, élevées, moyennes, faibles ou indicatives, du plus grave au moins grave. Le niveau de gravité d'un groupe est égal au résultat de gravité le plus élevé parmi les résultats de ce groupe.

Les groupes contenant des résultats critiques ou de niveau de gravité élevé ayant un impact sur un grand nombre d'entités doivent être priorisés pour les enquêtes, car ils sont plus susceptibles de représenter des problèmes de sécurité à fort impact.

Titre du groupe

Dans la colonne Titre, chaque groupe possède un identifiant unique et un titre non unique. Ils sont basés sur le ASFF type d'espace de noms du groupe et sur le nombre de résultats contenus dans cet espace de noms dans le cluster. Par exemple, si un regroupement porte le titre suivant : Groupe avec : TTP(2), Effet (1) et Comportement inhabituel (2), il inclut cinq résultats au total, soit deux résultats dans l'espace de TTPnoms, un résultat dans l'espace de noms Effect et deux résultats dans l'espace de noms Unusual Behavior. Pour une liste complète des espaces de noms, consultez la section Taxonomie des types pour. ASFF

Tactiques d'un groupe

La colonne Tactiques d'un groupe détaille la catégorie de tactiques à laquelle appartient l'activité. Les catégories de tactiques, de techniques et de procédures de la liste suivante s'alignent sur la matrice MITRE ATT &CK.

Vous pouvez sélectionner une tactique sur la chaîne pour en voir la description. Après la chaîne se trouve une liste des tactiques détectées au sein du groupe. Ces catégories et les activités qu'elles représentent généralement sont les suivantes :

- Accès initial : un adversaire essaie de pénétrer dans le réseau de quelqu'un d'autre.
- Exécution : un adversaire essaie de pénétrer dans le réseau de quelqu'un d'autre.
- Persistance : un adversaire essaie de maintenir sa position.
- Escalade de privilèges : un adversaire essaie d'obtenir des autorisations de niveau supérieur.
- Évasion défensive : un adversaire essaie d'éviter d'être détecté.
- Accès aux informations d'identification : un adversaire essaie de voler des noms de compte et des mots de passe.
- Découverte : un adversaire essaie de comprendre un environnement et d'en apprendre davantage sur celui-ci.
- Mouvement latéral : un adversaire essaie de se déplacer dans un environnement.
- Collecte : un adversaire essaie de recueillir des données présentant un intérêt pour son objectif.
- Commande et contrôle : un adversaire essaie de s'introduire dans le réseau de quelqu'un d'autre.
- Exfiltration : un adversaire essaie de voler des données.
- Impact : un adversaire tente de manipuler, d'interrompre ou de détruire vos systèmes et vos données.
- Autre : indique une activité à partir d'un résultat qui ne correspond pas aux tactiques répertoriées dans la matrice.

Entités au sein d'un groupe

La colonne Entités contient des détails sur les entités spécifiques détectées au sein de ce groupe. Sélectionnez cette valeur pour une ventilation des entités en fonction des catégories : identité, réseau, stockage et calcul. Voici des exemples d'entités dans chaque catégorie :

- Identité : IAM principes et Comptes AWS, par exemple, utilisateur et rôle
- Réseau : adresse IP ou autre réseau et VPC entités
- Stockage : compartiments Amazon S3 ou DDBs
- EC2Instances de calcul Amazon ou conteneurs Kubernetes

Comptes au sein d'un groupe

La colonne Comptes indique à quels AWS comptes appartiennent les entités impliquées dans les résultats du groupe. Les AWS comptes sont répertoriés par nom et AWS identifiant afin que vous puissiez hiérarchiser les enquêtes sur les activités impliquant des comptes critiques.

Résultats au sein d'un groupe

La colonne Résultats contient une liste des entités d'un groupe par gravité. Les résultats incluent les résultats d'Amazon, GuardDuty les résultats d'Amazon Inspector, les résultats AWS de sécurité et les preuves de Detective. Vous pouvez sélectionner le graphe pour voir le nombre exact de résultats par gravité.

GuardDuty les résultats font partie du package principal de Detective et sont ingérés par défaut. Tous les autres résultats AWS de sécurité agrégés par Security Hub sont ingérés en tant que source de données facultative. Voir Données source utilisées dans un graphe de comportement pour plus de détails.

Résultats informatifs dans les groupes de résultats

Amazon Detective identifie des informations supplémentaires liées à un groupe de résultats sur la base des données de votre graphe de comportement collectées au cours des 45 derniers jours. Detective présente cette information comme un résultat ayant le niveau de sévérité informationnel. Les preuves fournissent des informations complémentaires qui mettent en évidence une activité inhabituelle ou un comportement inconnu potentiellement suspect au sein d'un groupe de résultats. Cela peut inclure des géolocalisations récemment observées ou des API appels observés dans le cadre d'une découverte. Les résultats des preuves ne sont visibles que dans Detective et ne sont pas envoyés à AWS Security Hub.

Detective détermine l'emplacement des demandes à l'aide des bases de MaxMind données GeoIP. MaxMind fait état d'une très grande précision de ses données au niveau des pays, bien que la précision varie en fonction de facteurs tels que le pays et le type de propriété intellectuelle. Pour plus d'informations MaxMind, consultez la section Géolocalisation MaxMind IP. Si vous pensez que l'une des données GeoIP est incorrecte, vous pouvez envoyer une demande de correction à Maxmind à l'adresse MaxMind Correct Geo Data. IP2

Vous pouvez observer des preuves pour différents types principaux (tels que IAM l'utilisateur ou IAM le rôle). Pour certains types de preuves, vous pouvez observer les preuves pour tous les comptes. Cela signifie que les preuves affectent l'ensemble de votre graphe de comportement. Si un résultat

probant est observé pour tous les comptes, vous verrez également au moins un résultat informatif supplémentaire du même type pour un IAM rôle individuel. Par exemple, si vous voyez un résultat Nouvelle géolocalisation observée pour tous les comptes, vous en verrez un autre pour Nouvelle géolocalisation observée pour un principal.

Types de preuves dans les groupes de résultats

- Nouvelle géolocalisation observée
- Nouvelle organisation du système autonome (ASO) observée
- Nouvel agent utilisateur observé
- Nouvel API appel émis
- Nouvelle géolocalisation observée pour tous les comptes
- Nouveau IAM principal observé pour tous les comptes

Profils de groupes de résultats

Lorsque vous sélectionnez le titre d'un groupe, un profil de groupe de résultats s'ouvre avec des informations supplémentaires sur ce groupe. Le volet de détails de la page de profil des groupes de résultats permet d'afficher jusqu'à 1 000 entités et résultats pour le parent et les enfants des groupes de résultats.

La page de profil du groupe affiche la durée de validité définie pour le groupe. Il s'agit de la date et de l'heure entre le premier résultat ou la première preuve inclus dans le groupe et le résultat ou preuve mis à jour le plus récemment dans un groupe. Vous pouvez également consulter la gravité du groupe de résultats, qui est égale à la catégorie de gravité la plus élevée parmi les résultats du groupe. Les autres détails de ce volet de profil incluent :

- La chaîne des tactiques impliquées vous indique quelles tactiques sont attribuées aux résultats du groupe. Les tactiques sont basées sur la matrice MITRE ATT &CK pour les entreprises. Les tactiques sont représentées sous la forme d'une chaîne de points colorés qui représente la progression typique d'une attaque, du stade le plus ancien au plus récent. Cela signifie que les cercles les plus à gauche de la chaîne représentent généralement des activités moins graves dans lesquelles un adversaire tente d'obtenir ou de conserver l'accès à votre environnement. À l'inverse, les activités menées vers la droite sont les plus graves et peuvent inclure la falsification ou la destruction de données.
- Les relations que ce groupe entretient avec d'autres groupes. Parfois, un ou plusieurs groupes de résultats précédemment non connectés peuvent être fusionnés dans un nouveau groupe

en fonction d'un lien récemment découvert, par exemple, un résultat impliquant des entités des groupes existants. Dans ce cas, Amazon Detective désactive les groupes parents et crée un groupe enfant. Vous pouvez retracer la lignée de n'importe quel groupe jusqu'à ses groupes parents. Les relations entre les groupes peuvent être les suivantes :

- Groupe de résultats enfants : un groupe de résultats créé lorsqu'un résultat impliqué dans deux autres groupes de résultats est impliqué dans un nouveau résultat. Les groupes parents du résultat sont répertoriés pour tous les groupes d'enfants.
- Groupe de résultats parents : un groupe de résultats est un parent lorsqu'un groupe d'enfants a été créé à partir de celui-ci. Si un groupe de résultats est un parent, les enfants concernés sont répertoriés avec celui-ci. Le statut d'un groupe de parents devient inactif lorsqu'il est fusionné avec un groupe d'enfants actif.

Deux onglets d'informations ouvrent les volets de profil. À l'aide des onglets Entités impliquées et Résultats impliqués, vous pouvez consulter des informations supplémentaires sur le groupe.

Utilisez Exécuter une enquête pour générer un rapport d'enquête. Le rapport généré détaille le comportement anormal qui indique une compromission.

Profil au sein des groupes

Entités impliquées

Se concentre sur les entités du groupe de résultats, notamment sur les résultats du groupe auxquels chaque entité est liée. Les balises associées à chaque entité sont également affichées afin que vous puissiez identifier rapidement les entités importantes en fonction du balisage. Sélectionnez une entité pour afficher son profil d'entité.

Résultats impliqués

Fournit des détails sur chaque résultat, y compris la gravité du résultat, chaque entité impliquée et la date à laquelle ce résultat a été observé pour la première et la dernière fois. Sélectionnez un type de résultat dans la liste pour ouvrir un volet des détails du résultat contenant des informations supplémentaires sur ce résultat. Dans le cadre du volet Résultats impliqués, vous pouvez voir des résultats informationnels basés sur les preuves Detective issues de votre graphe de comportement.

Visualisation de groupe de résultats

Amazon Detective fournit une visualisation interactive des groupes de résultats. Cette visualisation est conçue pour vous aider à étudier les problèmes plus rapidement et de manière plus approfondie avec moins d'efforts. Le volet de visualisation de groupe de résultats affiche les résultats et les entités impliquées dans un groupe de résultats. Vous pouvez utiliser cette visualisation interactive pour analyser, comprendre et trier l'impact du groupe de résultats. Ce volet permet de visualiser les informations présentées dans le tableau Entités impliquées et résultats impliqués. Dans la présentation visuelle, vous pouvez sélectionner des résultats ou des entités pour une analyse plus approfondie.

Les groupes de résultats Detectives contenant des résultats agrégés sont un cluster de résultats connectés au même type de ressource. Grâce aux résultats agrégés, vous pouvez rapidement évaluer la composition d'un groupe de résultats et interpréter les problèmes de sécurité plus rapidement. Dans le volet de détails des groupes de résultats, les résultats similaires sont combinés et vous pouvez développer les résultats pour afficher ensemble des résultats relativement similaires. Par exemple, il y a agrégation d'un nœud de preuves contenant des résultats informationnels et des résultats moyens du même type. À l'heure actuelle, vous pouvez consulter le titre, la source, le type et la gravité des groupes de résultats avec des résultats agrégés.

À partir de ce volet interactif, vous pouvez :

- Utilisez Exécuter une enquête pour générer un rapport d'enquête. Le rapport généré détaille les comportements anormaux qui indiquent une compromission. Pour plus de détails, consultez Detective Investigations.
- Consulter plus de détails sur les groupes de résultats avec des résultats agrégés pour analyser les preuves, les entités et les résultats concernés.
- Consulter les étiquettes des entités et les résultats afin d'identifier les entités concernées présentant des problèmes de sécurité potentiels. Vous pouvez désactiver l'étiquette.
- Réorganisez les entités et les résultats pour mieux comprendre leur interdépendance. Isolez les entités et les résultats d'un groupe en déplaçant l'élément sélectionné dans le groupe de résultats.
- Sélectionnez les preuves, les entités et les résultats pour obtenir plus de détails à leur sujet. Pour sélectionner plusieurs éléments, choisissez **`command/control`** ou faites-les glisser à l'aide du pointeur.
- Ajustez la mise en page pour adapter toutes les entités et résultats à la fenêtre du groupe de résultats. Découvrez quels types d'entités sont courants dans un groupe de résultats.

> **Note**
>
> Le volet de visualisation des groupes de résultats prend en charge l'affichage de groupes de résultats contenant jusqu'à 100 entités et résultats.

Vous pouvez utiliser le menu déroulant pour afficher les résultats et les entités dans une mise en page radiale, circulaire, dirigée par force ou en grille. La disposition radiale fournit une meilleure visualisation pour faciliter l'interprétation des données. La mise en page dirigée par force positionne les entités et les résultats de manière à ce que les liens aient une longueur constante entre les éléments, et que les liens soient répartis uniformément. Cela permet de réduire les chevauchements. La mise en page que vous sélectionnez définit le placement des résultats dans le volet Visualisation.

Disposition chronologique

La mise en page chronologique fournit un moyen dynamique de visualiser l'évolution de vos groupes de recherche au fil du temps. Cela vous permet de suivre la progression des événements, ce qui vous aide à mieux comprendre la séquence et la causalité potentielle des incidents de sécurité à l'aide de Detective.

Utilisez le curseur de chronologie situé en bas du panneau de visualisation pour sélectionner un point précis dans le temps. La visualisation sera mise à jour pour afficher l'état de votre groupe de recherche à ce moment-là. Le bouton de lecture qui vous permet de progresser automatiquement dans la chronologie. Cliquez sur le bouton de lecture pour démarrer l'animation. La visualisation sera mise à jour en temps réel, indiquant l'évolution du groupe de recherche au fil du temps. Utilisez le bouton pause pour arrêter l'animation à tout moment.

Vous pouvez désormais filtrer les résultats en fonction de leur niveau de gravité à l'aide de la liste déroulante Filtre. Lorsque vous appliquez un filtre, la visualisation est mise à jour pour afficher uniquement les résultats correspondant au niveau de gravité sélectionné. Le filtre affecte uniquement les résultats affichés dans la chronologie, et non dans la visualisation complète du groupe de recherche. Cela vous permet de vous concentrer rapidement sur les problèmes prioritaires ou d'étudier des types de résultats spécifiques.

Vous pouvez utiliser la fonction de filtrage en combinaison avec la mise en page chronologique pour voir comment les résultats de différents niveaux de gravité apparaissent et évoluent au fil du temps.

Flux de travail d'investigation amélioré

Grâce à l'ajout de la mise en page chronologique et des fonctionnalités de filtrage, vous pouvez désormais mener des enquêtes encore plus complètes :

1. Commencez par visualiser l'ensemble du groupe de recherche à l'aide de l'une des mises en page statiques (radiale, circulaire, dirigée par force ou grille).
2. Utilisez des chronologies pour comprendre l'évolution de la situation au fil du temps.
3. Utilisez le bouton de lecture pour progresser automatiquement dans la chronologie, en surveillant les moments ou les modèles clés.
4. Faites une pause à des points importants pour approfondir vos recherches.
5. Appliquez des filtres pour vous concentrer sur les résultats présentant des niveaux de gravité spécifiques.
6. Utilisez les raccourcis clavier et les outils de sélection pour approfondir les entités et les résultats qui vous intéressent.

Ce flux de travail amélioré permet une étude plus nuancée et approfondie de scénarios de sécurité complexes. Vous pouvez mener des enquêtes de sécurité plus efficaces, ce qui permet de résoudre plus rapidement les incidents et d'améliorer la posture de sécurité globale.

Raccourcis clavier

Vous pouvez utiliser les raccourcis clavier suivants pour interagir avec le panneau de visualisation du groupe de recherche :

- Cliquez — Sélectionne un seul nœud, désélectionne tous les autres nœuds, désélectionne tous les nœuds si vous cliquez sur un espace blanc.
- Ctrl + Clic — Sélectionne un seul nœud, mais ne désélectionne pas les autres nœuds.
- Faire glisser — Déplace la vue.
- Ctrl + Drag — Marquee sélectionne les autres nœuds, mais ne les désélectionne pas.
- Shift + Drag — Marquee sélectionne et désélectionne tous les autres nœuds.
- Touches fléchées — Modifie le focus entre les nœuds.
- Ctrl + Espace — Sélectionne ou désélectionne le nœud actuellement ciblé.
- Touches Shift + Flèches — Modifie le focus entre les nœuds et les sélectionne.

La légende dynamique change en fonction des entités et des résultats de votre graphe actuel. Elle vous aide à identifier ce que représente chaque élément visuel.

Récapitulatif des groupes de résultats optimisé par l'IA générative

Par défaut, Amazon Detective fournit automatiquement des récapitulatifs d'un groupe de résultats individuel. Les récapitulatifs sont basés sur des modèles d'intelligence artificielle générative (IA générative) hébergés sur Amazon Bedrock.

En utilisant des groupes de résultats, vous pouvez examiner plusieurs résultats de sécurité, dans la mesure où ils se rapportent à un événement de sécurité potentiel, et identifier les acteurs potentiels de la menace. Les récapitulatifs de groupes de résultats pour les groupes de résultats s'appuient sur ces fonctionnalités. Les récapitulatifs de groupes de résultats consomment les données d'un groupe de résultats, analysent rapidement les relations entre les résultats et les ressources affectées, puis résument les menaces potentielles en langage naturel. Vous pouvez utiliser ces récapitulatifs pour identifier les menaces de sécurité les plus importantes, améliorer l'efficacité des enquêtes et raccourcir les délais de réponse.

> **Note**
>
> Les récapitulatifs de groupes de résultats optimisés par l'IA générative peuvent fournir des informations totalement précises, mais pas toujours. Consultez .AWS Politique en matière d'IA responsable pour plus d'informations.

Examen du récapitulatif du groupe de résultats

Le récapitulatif d'un groupe de résultats fournit une explication claire et détaillée d'un événement de sécurité. En langage naturel, l'explication comprend un titre succinct, un récapitulatif des ressources impliquées et des informations organisées sur ces ressources.

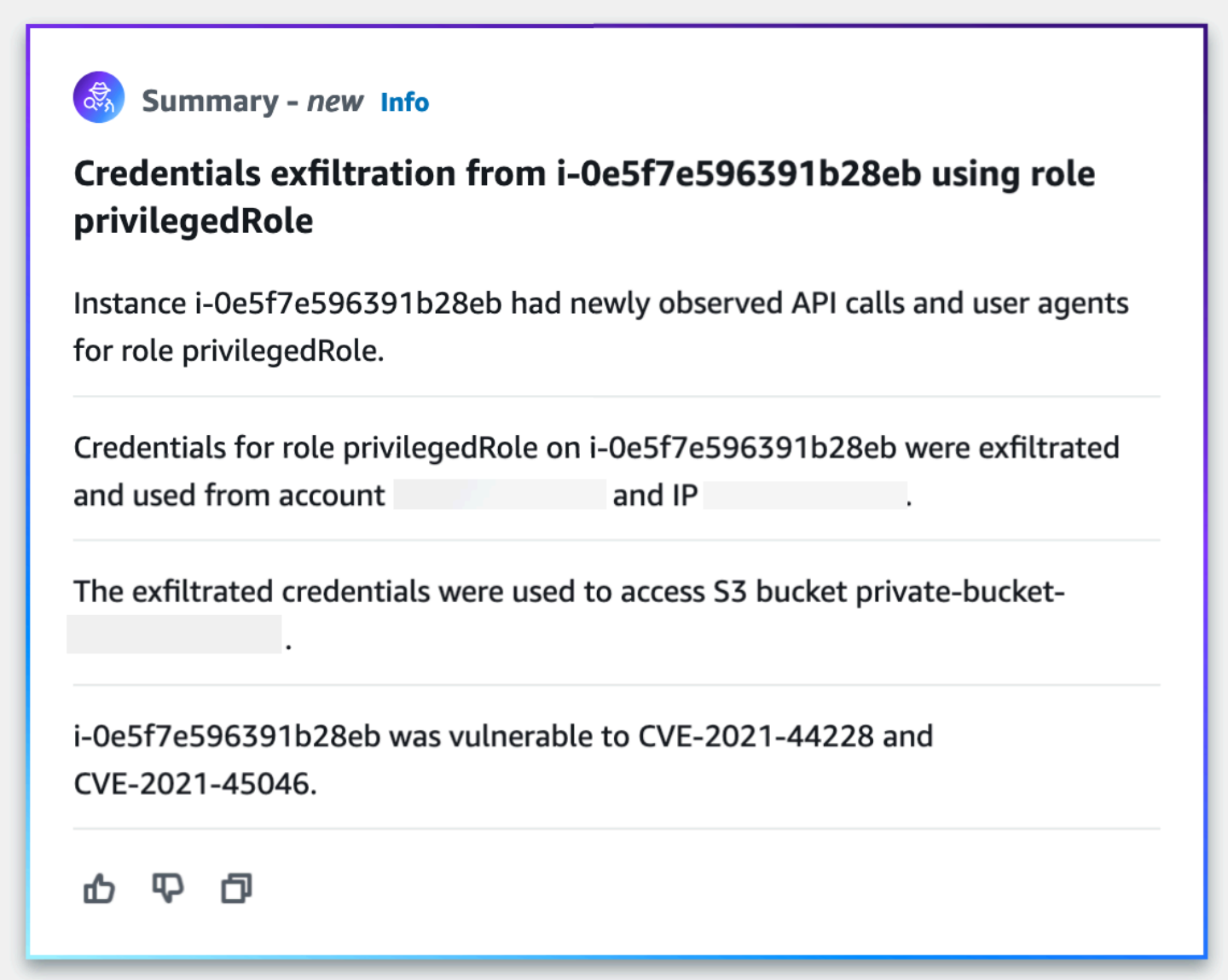
Pour consulter le résumé d'un groupe de résultats

1. Ouvrez la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, choisissez Groupes de résultats.
3. Dans le tableau groupes de résultats, choisissez le groupe de résultats dont vous souhaitez afficher un récapitulatif. Une page de détails s'affiche.

Sur la page de détails, vous pouvez utiliser le volet Récapitulatif pour consulter un récapitulatif descriptif généré des principaux résultats du groupe de résultats. Vous pouvez également consulter

une analyse des principaux événements constituant une menace dans le groupe de résultats, que vous pourrez ensuite approfondir. Pour ajouter le résumé généré à vos notes ou à un système de billetterie, cliquez sur l'icône de copie dans le volet. Cette action copie le récapitulatif dans votre presse-papiers. Vous pouvez également partager vos commentaires sur le récapitulatif du groupe de résultats dans le récapitulatif, ce qui peut améliorer l'expérience à l'avenir. Pour partager vos commentaires, cliquez sur l'icône du pouce vers le haut ou du pouce vers le bas, selon la nature de vos commentaires.

> **Note**
>
> Si vous fournissez des commentaires sur le récapitulatif du groupe de résultats, ils ne sont pas utilisés pour le réglage du modèle. Nous l'utilisons uniquement pour garantir que les instructions de Detective sont conçues de manière efficace.



Désactivation du récapitulatif des groupes de résultats

Par défaut, le récapitulatif des groupes de résultats est activé pour les groupes de résultats. Vous pouvez désactiver à tout moment le récapitulatif du groupe de résultats. Si vous le désactivez, vous pouvez le réactiver ultérieurement.

Pour désactiver le récapitulatif du groupe de résultats

1. Ouvrez la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, sélectionnez Préférences.
3. Sous Récapitulatif du groupe de résultats, choisissez Modifier.
4. Désactivez Activé.

5. Choisissez Enregistrer.

Activation du récapitulatif des groupes de résultats

Si vous avez précédemment désactivé le récapitulatif des groupes de résultats pour les groupes de résultats, vous pouvez les activer de nouveau à tout moment.

Pour activer le récapitulatif des groupes de résultats

1. Ouvrez la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, sélectionnez Préférences.
3. Sous Récapitulatif du groupe de résultats, choisissez Modifier.
4. Activez Activé.
5. Choisissez Enregistrer.

Régions prises en charge

Le résumé du groupe de recherche est disponible ci-dessous AWS Régions.

- USA Est (Virginie du Nord)
- USA Ouest (Oregon)
- Asie-Pacifique (Tokyo)
- Europe (Francfort)

Archivage d'une recherche sur Amazon GuardDuty

Lorsque vous avez terminé votre enquête sur un GuardDuty résultat d'Amazon, vous pouvez archiver le résultat auprès d'Amazon Detective. Cela vous évite d'avoir à revenir à pour effectuer la mise à jour. GuardDuty L'archivage d'un résultat indique que vous avez terminé votre enquête à son sujet.

Vous ne pouvez archiver une GuardDuty découverte depuis Detective que si vous êtes également le compte GuardDuty administrateur du compte associé à la découverte. Si vous n'êtes pas un compte GuardDuty administrateur et que vous tentez d'archiver un résultat, un message d'erreur GuardDuty s'affiche.

Pour archiver une GuardDuty découverte

1. Connectez-vous à la console AWS de gestion. Ouvrez ensuite la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans la console Detective, dans le volet des détails des résultats, choisissez Résultat d’archive.
3. Lorsque vous êtes invité à confirmer, choisissez Archive.

Vous pouvez consulter les GuardDuty résultats archivés dans la GuardDuty console. Les résultats archivés sont conservés GuardDuty pendant 90 jours et peuvent être consultés à tout moment pendant cette période. Vous pouvez afficher les résultats supprimés dans la GuardDuty console en sélectionnant Archivé dans le tableau des résultats ou GuardDuty API en utilisant le ListFindingsAPIfindingCriteriacritère service.archivé égal à true. Pour en savoir plus, consultez les règles de suppression dans le guide de GuardDuty l'utilisateur Amazon.

Analyse des entités dans Amazon Detective

Une entité est un objet unique extrait des données sources. Les exemples incluent une adresse IP, une EC2 instance Amazon ou un AWS compte spécifique. Consultez the section called "Types d'entités dans la structure de données du graphe de comportement" pour obtenir la liste des types d'entités.

Le profil d'une entité Amazon Detective est une page unique qui fournit des informations détaillées sur l'entité et son activité. Vous pouvez utiliser un profil d'entité pour obtenir des informations complémentaires d'une enquête sur un résultat ou dans le cadre d'une recherche générale d'activités suspectes.

Table des matières

- Utilisation de profils d'entités
- Affichage et interaction avec les panneaux de profil de Detective
- Accès direct au profil d'une entité ou d'une vue d'ensemble des résultats
- Pivotement d'un volet de profil vers une autre console
- Exploration des détails d'activité sur un volet de profil
- Gestion de la durée de validité
- Afficher les détails des résultats associés dans Detective
- Afficher les détails des entités à volume élevé dans Detective

Utilisation de profils d'entités

Un profil d'entité apparaît lorsque vous effectuez une des actions suivantes :

- Dans la GuardDuty console Amazon, choisissez l'option permettant d'étudier une entité associée à un résultat sélectionné.

  veuillez consulter the section called "Pivotement depuis une autre console".
- Accédez à l'URL Detective correspondant au profil de l'entité.

  veuillez consulter the section called "Navigation à l'aide d'une URL".
- Utilisez la recherche Detective dans la console Detective pour rechercher une entité.

- Choisissez un lien vers le profil d'entité à partir d'un autre profil d'entité ou d'une vue d'ensemble des résultats.

Durée de validité d'un profil d'entité

Lorsque vous accédez directement au profil d'une entité sans indiquer la durée de validité, celle-ci est définie aux 24 heures précédentes.

Lorsque vous naviguez vers un profil d'entité à partir d'un autre profil d'entité, la durée de validité actuellement sélectionnée reste inchangée.

Lorsque vous accédez à un profil d'entité à partir d'une vue d'ensemble des résultats, la durée de validité est définie en fonction de la fenêtre temporelle de résultats.

Pour plus d'informations sur la personnalisation de la durée du champ d'application afin de limiter les données affichées sur les profils d'entité, consultez la section Gestion de la durée du champ d'application.

Identifiant et type d'entité

L'identifiant de l'entité et le type d'entité se trouvent en haut du profil. Chaque type d'entité possède une icône correspondante, afin de fournir un indicateur visuel du type de profil.

Résultats impliqués

Chaque profil contient une liste des résultats impliquant l'entité pendant la période de validité.

Vous pouvez voir les détails de chaque résultat, modifier la durée de validité pour refléter la fenêtre temporelle de résultats, et accéder à la vue d'ensemble des résultats pour rechercher d'autres ressources impliquées.

veuillez consulter the section called "Affichage des résultats d'une entité".

Groupes de résultats impliquant cette entité

Chaque profil contient une liste de groupes de résultats dans lesquels une entité est incluse.

Un groupe de résultats est composé de résultats, d'entités et de preuves que Detective rassemble dans un groupe afin de fournir plus de contexte sur d'éventuels problèmes de sécurité.

Pour plus d'informations sur les groupes de résultats, consultez the section called "Trouver des groupes".

Volets de profil contenant les détails des entités et les résultats d'analyse

Chaque profil d'entité contient un groupe d'un ou de plusieurs onglets. Chaque onglet contient un ou plusieurs volets de profil. Chaque volet de profil contient du texte et des visualisations générés à partir des données du graphe de comportement. Les onglets et volets de profil spécifiques sont adaptés au type d'entité.

Pour la plupart des entités, le volet situé en haut du premier onglet fournit des informations récapitulatives de haut niveau sur l'entité.

D'autres volets de profil mettent en évidence différents types d'activités. Pour une entité impliquée dans un résultat, les informations figurant dans les volets de profil de l'entité peuvent fournir des preuves supplémentaires pour aider à mener à bien une enquête. Chaque volet de profil donne accès à des instructions sur la manière d'utiliser les informations. Pour plus d'informations, consultez the section called "Utilisation des instructions du volet de profil".

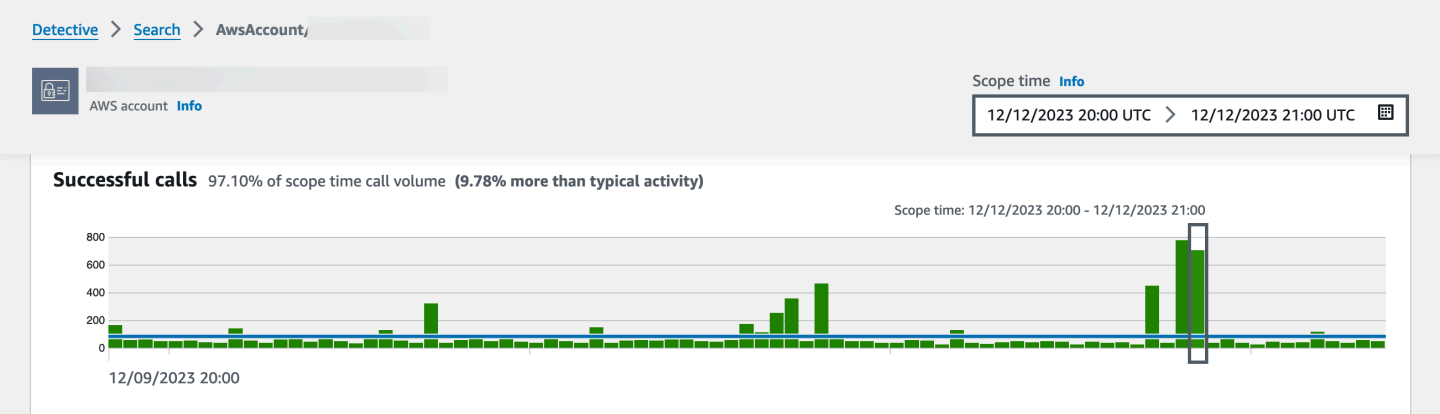
Pour plus de détails sur les volets de profil, les types de données qu'ils contiennent et les options disponibles pour interagir avec eux, consultez the section called "Panneaux profilés".

Naviguer dans un profil d'entité

Un profil d'entité contient un ensemble d'un ou de plusieurs onglets. Chaque onglet contient un ou plusieurs volets de profil. Chaque volet de profil contient du texte et des visualisations générés à partir des données du graphe de comportement.

Lorsque vous parcourez un onglet de profil vers le bas, les informations suivantes restent visibles en haut du profil :

- Type d'entité
- Identifiant d'entité.
- Durée de validité



Affichage et interaction avec les panneaux de profil de Detective

Chaque profil d'entité sur la console Amazon Detective se compose d'un ensemble de volets de profil. Un volet de profil est une visualisation qui fournit des détails généraux ou met en évidence une activité spécifique associée à une entité. Les volets de profil utilisent différents types de visualisations pour présenter différents types d'informations. Ils peuvent également fournir des liens vers des informations supplémentaires ou vers d'autres profils.

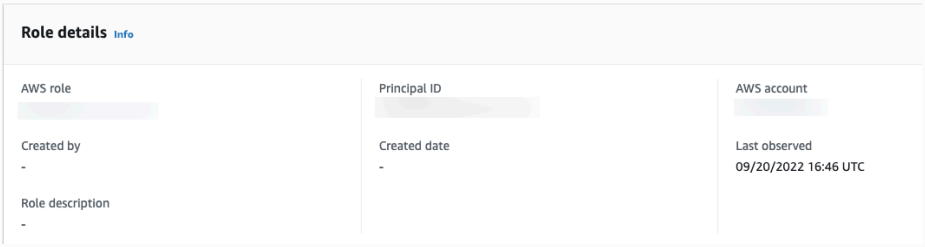
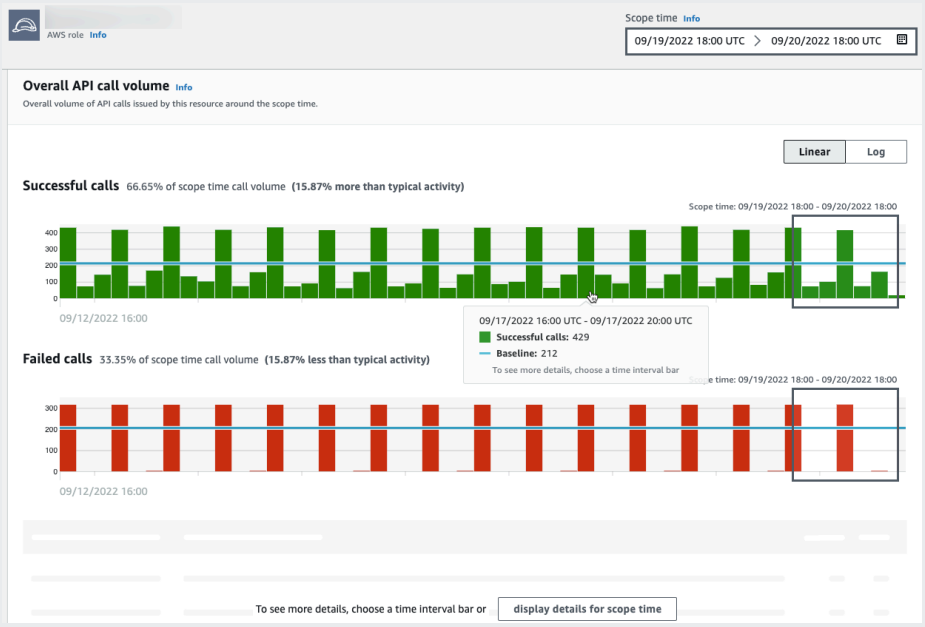
Chaque volet de profil est destiné à aider les analystes à trouver des réponses à des questions spécifiques concernant les entités et leurs activités associées. Les réponses à ces questions permettent de déterminer si l'activité représente une véritable menace.

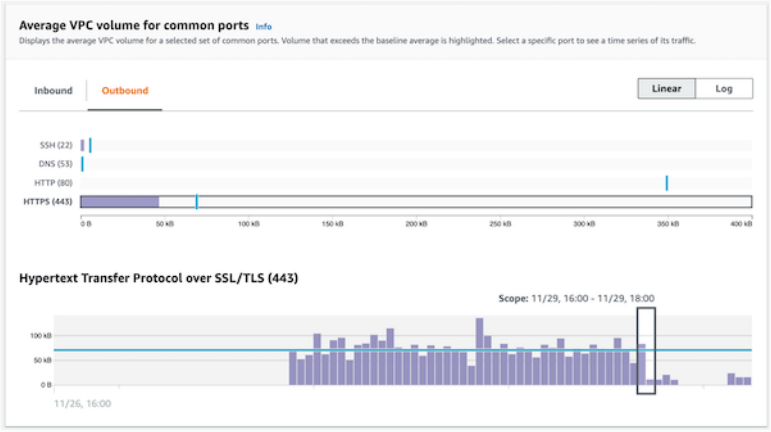
Les volets de profil utilisent différents types de visualisations pour présenter différents types d'informations.

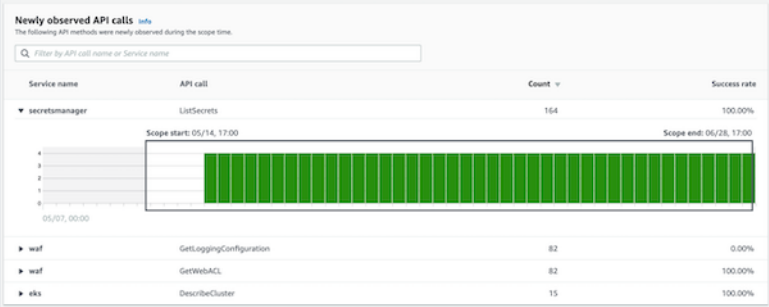
Types d'informations sur un volet de profil

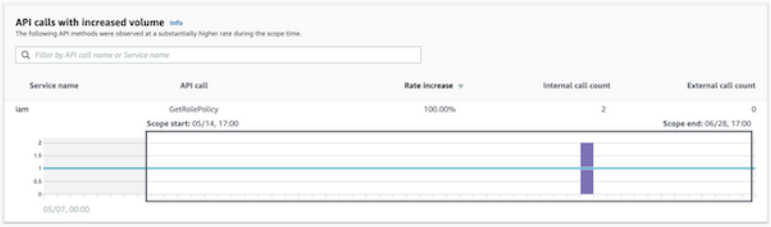
Les volets de profil fournissent généralement les types de données suivants.

Type de données du volet	Description
Informations de haut niveau sur un résultat ou une entité	Le type de volet le plus simple fournit quelques informations de base sur une entité. Les exemples d'informations incluses dans un volet d'informa tion incluent l'identifiant, le nom, le type et la date de création.

Type de données du volet	Description
	 La plupart des profils d'entité contiennent un volet d'informations pour cette entité.
Résumé général de l'activité au fil du temps	Affiche un résumé de l'activité d'une entité au fil du temps. Ce type de volet fournit une vue d'ensemble du comportement d'une entité pendant la période couverte par la durée de validité.  Voici quelques exemples de données récapitulatives fournies sur les volets de profil Detective : • APIAppels échoués et réussis • Volume entrant et sortant VPC

Type de données du volet	Description
Résumé de l'activité regroupée par valeurs	Affiche un résumé de l'activité d'une entité, regroupée selon des valeurs spécifiques. Vous pouvez voir ce type de panneau de profil sur le profil d'une EC2 instance. Le panneau de profil indique le volume moyen de données du journal de VPC flux à destination et en provenance d'une EC2 instance pour les ports courants associés à des types de services spécifiques. 

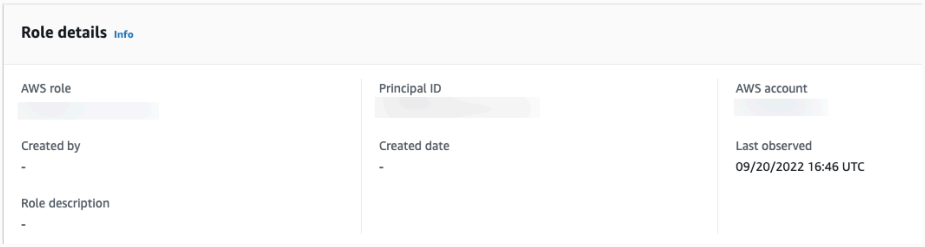
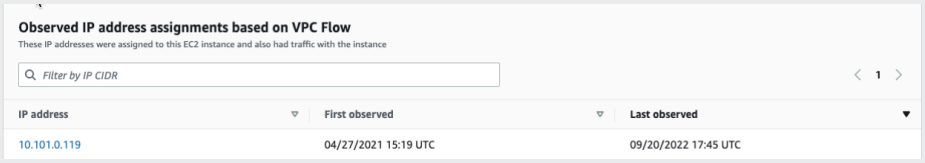
Type de données du volet	Description
Activité qui n'a débuté que pendant la durée de validité	Au cours d'une enquête, il est utile de voir quelle activité n'a commencé à se produire qu'au cours d'une période donnée. Par exemple, y a-t-il des API appels, des emplacements géographiques ou des agents utilisateurs qui n'ont jamais été vus auparavant ?  Si le graphe de comportement est toujours en mode apprentis sage, le volet de profil affiche un message de notification. Le message est supprimé lorsque le graphique de comportement a accumulé au moins deux semaines de données. Pour plus d'informations sur l'entraînement d'un modèle, consultez the section called "Période de formation pour les nouveaux graphes de comportement".

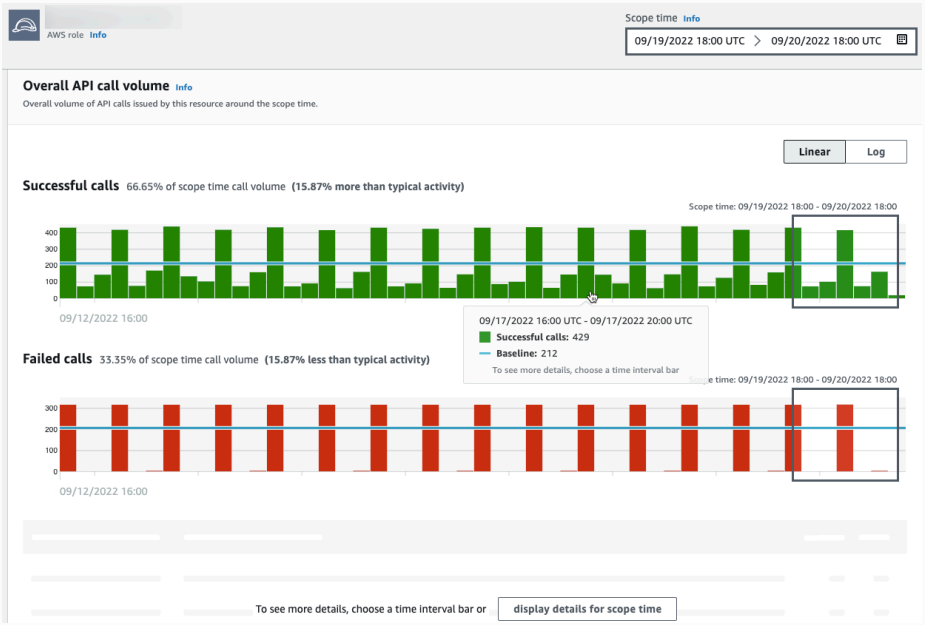
Type de données du volet	Description
Activité qui a changé de manière significative pendant la période couverte par la durée de validité	À l'instar des nouveaux volets d'activité, les volets de profil peuvent également afficher les activités qui ont changé de manière significative au cours de la période couverte par la durée de validité. Par exemple, un utilisateur peut régulièrement émettre un certain API appel plusieurs fois par semaine. Si le même utilisateur émet soudainement le même appel plusieurs fois au cours d'une même journée, cela peut être le signe d'une activité malveillante.  Si le graphe de comportement est toujours en mode apprentis sage, le volet de profil affiche un message de notification. Le message est supprimé lorsque le graphique de comportement a accumulé au moins deux semaines de données. Pour plus d'informations sur l'entraînement d'un modèle, consultez the section called "Période de formation pour les nouveaux graphes de comportement".

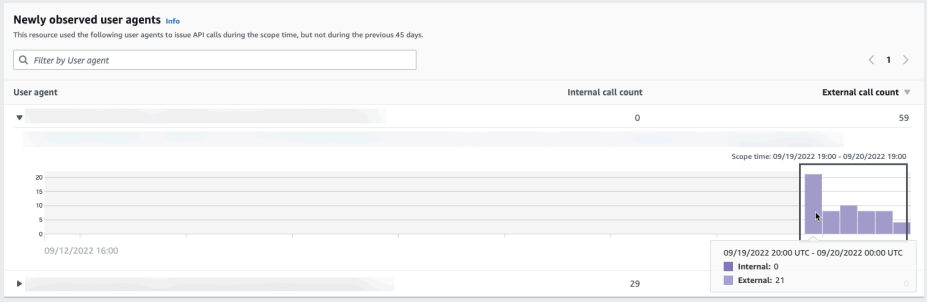
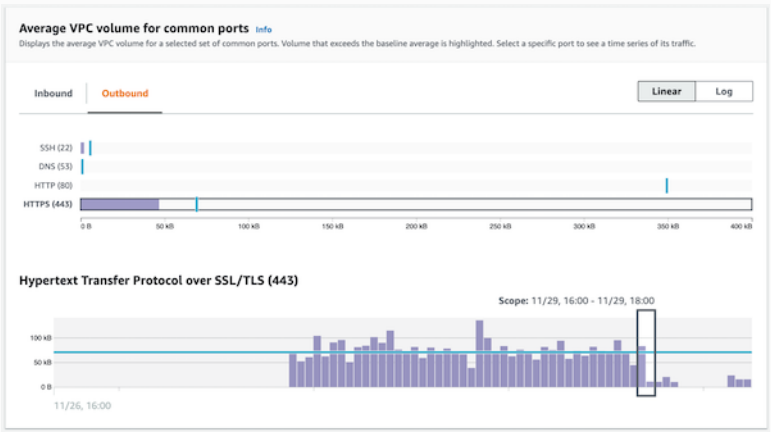
Types de visualisations du volet de profil

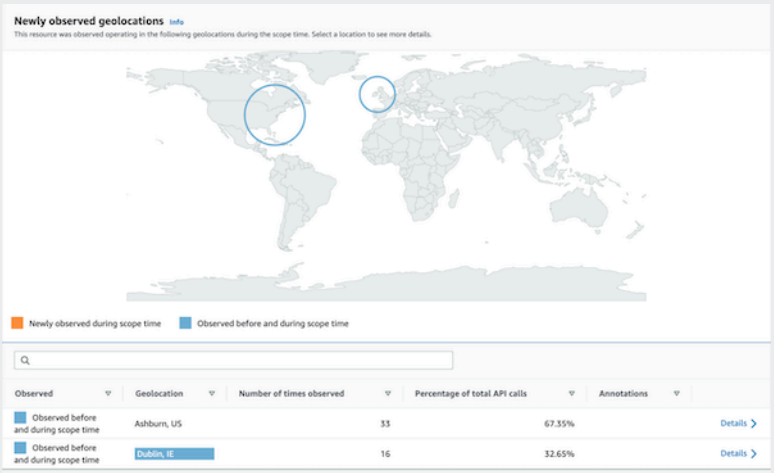
Le contenu du volet de profil peut prendre l'une des formes suivantes.

Type de visualisation	Description
Paires clé-valeur	Le type de visualisation le plus simple est un ensemble de paires clé-valeur. Un volet de résultat ou d'information sur les entités est l'exemple le plus courant de volet de paires clé-valeur.

Type de visualisation	Description
	 Les paires clé-valeur peuvent également être utilisées pour ajouter des informations supplémentaires à d'autres types de volets. À partir d'un volet de paires clé-valeur, si une valeur est l'identif iant d'une entité, vous pouvez passer à son profil.
Tableau	Un tableau est une simple liste d'éléments sur plusieurs colonnes.  Vous pouvez trier, filtrer et parcourir le tableau. Vous pouvez modifier le nombre d'entrées à afficher sur chaque page. Consultez the section called "Préférences pour les volets de profil". Si une valeur de la table est l'identifiant d'une entité, vous pouvez passer à son profil.

Type de visualisation	Description
Chronologie	Une visualisation chronologique présente une valeur agrégée pour des intervalles définis au fil du temps.  La chronologie met en évidence la durée de validité actuelle et inclut le temps périphérique supplémentaire avant et après la durée de validité. Le temps périphérique fournit le contexte de l'activité dans la durée de validité. Passez le pointeur de la souris sur un intervalle de temps pour afficher un récapitulatif des données relatives à cet intervalle de temps.

Type de visualisation	Description
Tableau extensible	Un tableau extensible combine des tableaux et des chronologies.  La visualisation commence sous la forme d'un tableau. Vous pouvez trier, filtrer et parcourir le tableau. Vous pouvez modifier le nombre d'entrées à afficher sur chaque page. Consultez the section called "Préférences pour les volets de profil". Vous pouvez ensuite développer chaque ligne pour afficher une visualisation chronologique spécifique à cette ligne.
Diagramme à barres	Un diagramme à barres montre les valeurs basées sur des groupements. En fonction du diagramme, vous pouvez être en mesure de choisir une barre pour afficher la chronologie des activités associées. 

Type de visualisation	Description
Diagramme de géolocalisation	Un diagramme de géolocalisation affiche une carte marquée pour mettre en évidence les données en fonction de l'emplace ment géographique. Il peut être suivi d'un tableau contenant des détails sur les différentes géolocalisations.  Notez que lors du traitement des données géographiques entrantes, Detective arrondit les valeurs de latitude et de longitude à une seule décimale.

Remarques sur le contenu du panneau de profil

Lors de la consultation du contenu d'un volet de profil, tenez compte des éléments suivants :

Avertissement relatif aux données de comptage approximatif

Cet avertissement indique que les éléments dont le nombre est extrêmement faible n'apparaissent pas en raison du volume de données applicables.

Pour garantir un comptage précis, réduisez la quantité de données. Le moyen le plus simple d'y parvenir est de réduire la durée de validité. Consultez the section called "Gestion de la durée de validité".

Arrondi pour les emplacements géographiques

Detective arrondit toutes les valeurs de latitude et de longitude à une seule décimale.

Modifications apportées à la façon dont Detective représente API les appels

À compter du 14 juillet 2021, Detective suit le service qui a effectué chaque API appel. Chaque fois que Detective affiche une API méthode, il affiche également le service associé. Sur les panneaux de profil qui affichent des informations sur les API appels, les appels sont toujours regroupés par service. Pour les données ingérées par Detective avant cette date, le nom du service est répertorié en tant que Service inconnu.

À compter du 14 juillet 2021, pour les comptes et les rôles, les détails de l'activité du panneau de profil du volume global d'APIappels n'indiquent plus le nom AKID de la ressource à l'origine de l'appel. Pour les comptes, Detective affiche l’identifiant du principal (utilisateur ou rôle) qui a émis l’appel. Pour les rôles, Detective affiche l’identifiant de la session de rôle. Pour les données ingérées par Detective avant le 14 juillet 2021, l’identifiant est répertorié comme ressource inconnue.

Pour les panneaux de profil qui affichent une liste d'APIappels, la chronologie associée met en évidence la période pendant laquelle cette transition s'est produite. La mise en évidence commence le 14 juillet 2021 et se termine lorsque la mise à jour a été entièrement propagée dans Detective.

Configuration des préférences pour un volet de profil

Pour les panneaux de profil, vous pouvez personnaliser le nombre de lignes qui apparaissent sur chaque page des panneaux de profil et configurer la préférence de format d'horodatage.

Définition de la longueur du tableau

Pour les volets de profil contenant des tableaux ou des tableaux extensibles, vous pouvez configurer le nombre de lignes à afficher sur chaque page.

Définissez vos préférences quant au nombre d’entrées sur chaque page.

1. Ouvrez la console Amazon Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, sous Paramètres, choisissez Préférences.
3. Sur la page Préférences, sous Longueur de la table, cliquez sur Modifier.
4. Choisissez le nombre de lignes de tableau que vous souhaitez afficher sur chaque page.
5. Choisissez Save (Enregistrer).

Définition du format d'horodatage

Pour les panneaux de profil, vous pouvez configurer la préférence de format d'horodatage qui sera appliquée à tous les horodatages de chaque IAM utilisateur ou rôle dans IAM Detective.

> **Note**
>
> La préférence de format d'horodatage n'est pas appliquée à l'ensemble AWS du compte.

Définissez la préférence pour l'horodatage.

1. Ouvrez la console Amazon Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, sous Paramètres, choisissez Préférences.
3. Sur la page Préférences, sous Préférences d'horodatage, affichez et modifiez l'affichage préféré pour tous les horodatages.
4. Par défaut, le format d'horodatage est défini sur. UTC Cliquez sur Modifier pour choisir votre fuseau horaire local.

   Exemple :

   Example

   UTC- 20/09/22 16h39 UTC

   Local - 20/09/2022 9:39 (- 07:00) UTC
5. Choisissez Save (Enregistrer).

Accès direct au profil d'une entité ou d'une vue d'ensemble des résultats

Pour accéder directement au profil d'une entité ou une vue d'ensemble des résultats dans Amazon Detective, vous pouvez utiliser l'une de ces options.

- Depuis Amazon GuardDuty ou depuis Amazon AWS Security Hub, vous pouvez passer d'une GuardDuty recherche au profil de recherche Detective correspondant.

- Vous pouvez créer une URL Detective qui identifie un résultat ou une entité et définit la durée de validité à utiliser.

En passant au profil d'une entité ou en trouvant une vue d'ensemble sur Amazon GuardDuty ou AWS Security Hub

Depuis la GuardDuty console Amazon, vous pouvez accéder au profil d'entité d'une entité associée à une découverte.

À partir des AWS Security Hub consoles GuardDuty et, vous pouvez également accéder à une vue d'ensemble des recherches. Cela fournit également des liens vers les profils d'entité des entités impliquées.

Ces liens peuvent aider à rationaliser le processus d'enquête. Vous pouvez rapidement utiliser Detective pour voir l'activité de l'entité associée et déterminer les prochaines étapes. Vous pouvez ensuite archiver un résultat s'il s'agit d'un faux positif ou l'explorer davantage pour déterminer l'ampleur du problème.

Comment passer à la console Amazon Detective

Les liens d'enquête sont disponibles pour tous les GuardDuty résultats. GuardDuty vous permet également de choisir d'accéder au profil d'une entité ou à l'aperçu des résultats.

Pour passer à Detective depuis la GuardDuty console

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Le cas échéant, choisissez Résultats dans le volet de navigation de gauche.
3. Sur la GuardDuty page Résultats, sélectionnez le résultat.

   Le volet des détails des résultats s'affiche à droite de la liste des résultats.
4. Dans le volet des détails de la recherche, choisissez Investigate in Detective.

   GuardDuty affiche la liste des éléments disponibles à étudier dans Detective.

   La liste contient à la fois les entités associées, telles que les adresses IP ou les instances EC2, et le résultat.
5. Choisissez une entité ou le résultat.

La console Detective s'ouvre dans un nouvel onglet. La console s'ouvre sur l'entité ou le profil de résultat.

Si vous n'avez pas activé Detective, la console s'ouvre sur une page d'accueil qui fournit une vue d'ensemble de Detective. À partir de là, vous pouvez choisir d'activer Detective.

Pour passer à Detective depuis la console Security Hub

1. Ouvrez la AWS Security Hub console à l'adresse https://console.aws.amazon.com/securityhub/.
2. Le cas échéant, choisissez Résultats dans le volet de navigation de gauche.
3. Sur la page Security Hub Findings, choisissez un GuardDuty résultat.
4. Dans le volet d'informations, choisissez Investigate in Detective, puis Investigate finding.

   Lorsque vous choisissez Investigate finding, la console Detective s'ouvre dans un nouvel onglet. La console s'ouvre pour afficher la vue d'ensemble des résultats.

   La console Detective s'ouvre toujours sur la région d'où provient le résultat, même si vous changez de région d'agrégation. Pour plus d'informations sur l'agrégation de résultat, consultez la section Agrégation des résultats par régions dans le guide de AWS Security Hub l'utilisateur.

   Si vous n'avez pas activé Detective, la console s'ouvre sur la page d'accueil de Detective. À partir de là, vous pouvez activer Detective.

Dépannage du pivot

Pour utiliser le pivot, l'une des conditions suivantes doit être vraie :

- Votre compte doit être un compte administrateur à la fois pour Detective et pour le service que vous quittez.
- Vous avez assumé un rôle multicompte qui vous permet d'accéder au graphe de comportement en tant qu'administrateur.

Pour plus d'informations sur la recommandation d'aligner les comptes administrateurs, consultez Alignement recommandé avec Amazon GuardDuty et AWS Security Hub.

Si le pivot ne fonctionne pas, vérifiez les points suivants.

- Le résultat appartient-il à un compte membre activé dans votre graphe de comportement ? Si le compte associé n'a pas été invité au graphe de comportement en tant que compte membre, le graphe de comportement ne contient aucune donnée pour ce compte.

  Si le compte d'un membre invité n'a pas accepté l'invitation, le graphe de comportement ne contient aucune donnée pour ce compte.
- Le résultat est-il archivé ? Detective ne reçoit pas les résultats archivés de GuardDuty.
- Le résultat a-t-il eu lieu avant que Detective ne commence à ingérer des données dans votre graphe de comportement ? Si le résultat n'est pas présent dans les données ingérées par Detective, le graphe de comportement ne contient aucune donnée correspondante.
- Le résultat provient-il de la bonne région ? Chaque graphe de comportement est spécifique à une région. Un graphe de comportement ne contient pas de données provenant d'autres régions.

Accès au profil d'une entité ou d'une vue d'ensemble des résultats à l'aide d'une URL

Pour accéder au profil d'une entité ou une vue d'ensemble des résultats dans Amazon Detective, vous pouvez utiliser une URL qui fournit un lien direct vers celui-ci. L'URL identifie le résultat ou l'entité. Il peut également spécifier la durée de validité à utiliser sur le profil. Detective conserve jusqu'à un an de données historiques sur les événements.

Format de l'URL d'un profil

> **Note**
>
> Si vous utilisez l'ancien format d'URL, Detective redirige automatiquement vers la nouvelle URL. L'ancien format de l'URL était le suivant : https://console.aws.amazon.com/detective/home?region=*Région*#*type*/*espace de noms*/*ID d'instance*?*paramètres*

Le nouveau format de l'URL du profil est le suivant :

- Pour les entités : https://console.aws.amazon.com/detective/home?region=*Région*#*entités*/*espace de noms*/*ID d'instance*?*paramètres*
- Pour les résultats : https://console.aws.amazon.com/detective/home?region=*Région*#*résultats*/*ID d'instance*?*paramètres*

L'URL nécessite les valeurs suivantes.

Région

La région que vous souhaitez utiliser.

type

Type d'élément correspondant au profil vers lequel vous naviguez.

- `entities` : indique que vous naviguez vers un profil d'entité
- `findings` : indique que vous naviguez vers une vue d'ensemble des résultats

espace de nom

Pour les entités, l'espace de noms est le nom du type d'entité.

- `AwsAccount`
- `AwsRole`
- `AwsRoleSession`
- `AwsUser`
- `Ec2Instance`
- `FederatedUser`
- `IpAddress`
- `S3Bucket`
- `UserAgent`
- `FindingGroup`
- `KubernetesSubject`
- `ContainerPod`
- `ContainerCluster`
- `ContainerImage`

ID d'instance

Identifiant d'instance du résultat ou de l'entité.

- Dans le cas d'une GuardDuty recherche, l'identifiant GuardDuty de la recherche.
- Pour un AWS compte, l'identifiant du compte.
- Pour AWS les rôles et les utilisateurs, l'identifiant principal du rôle ou de l'utilisateur.

- Pour les utilisateurs fédérés, l'identifiant principal de l'utilisateur fédéré. L'identifiant principal est *<identityProvider>*:*<username>* ou *<identityProvider>*:*<audience>*:*<username>*.
- Pour les adresses IP, l'adresse IP.
- Pour les agents utilisateurs, le nom de l'agent utilisateur.
- Pour les instances EC2, il s'agit de l'ID d'instance EC2.
- Pour les sessions de rôle, identifiant de session. L'identifiant de session utilise le format *<rolePrincipalID>*:*<sessionName>*.
- Pour les compartiments S3, le nom du compartiment.
- Pour un UUID FindingGroups, par exemple, `ca6104bc-a315-4b15-bf88-1c1e60998f83`
- Pour les ressources EKS, utilisez les formats suivants :
  - Cluster EKS : *<clusterName>~<accountId>~EKS*
  - *Module Kubernetes : ~ ~ ~EKS* <podUid><clusterName><accountId>
  - Sujet Kubernetes : *<subjectName>~<clusterName>~<accountId>*
  - Image du conteneur : *<registry>/<repository>:<tag>@<digest>*

Le résultat ou l'entité doit être associé à un compte activé dans votre graphe de comportement.

L'URL peut également inclure les paramètres facultatifs suivants, qui sont utilisés pour définir la durée de validité. Pour plus d'informations sur la durée de validité et son utilisation sur les profils, consultez the section called "Gestion de la durée de validité".

`scopeStart`

Heure de début de la durée de validité d'utilisation de l'oscilloscope sur le profil. L'heure de début doit se situer dans les 365 derniers jours.

La valeur est l'horodatage de l'époque.

Si vous indiquez une heure de début mais pas d'heure de fin, la durée de validité se termine à l'heure actuelle.

`scopeEnd`

Heure de fin de la durée de validité d'utilisation de l'oscilloscope sur le profil.

La valeur est l'horodatage de l'époque.

Si vous indiquez une heure de fin, mais pas d'heure de début, la durée de validité inclut tout le temps écoulé avant l'heure de fin.

Si vous ne spécifiez pas la durée de validité, c'est la durée de validité par défaut qui est utilisée.

- Pour les résultats, la durée de validité par défaut utilise la première et la dernière fois que l'activité de résultat a été observée.
- Pour les entités, la durée de validité par défaut correspond aux 24 heures précédentes.

Voici un exemple d'URL de Detective :

```
https://console.aws.amazon.com/detective/home?region=us-east-1#entities/
IpAddress/192.168.1.1?scopeStart=1552867200&scopeEnd=1552910400
```

Cet exemple d'URL fournit les instructions suivantes.

- Affichez le profil d'entité pour l'adresse IP 192.168.1.
- Utilisez une durée de validité qui commence le lundi 18 mars 2019 à 12:00:00 GMT et qui se termine le lundi 18 mars 2019 à 00h00 GMT.

Résolution des problèmes d'une règle

Si l'URL n'affiche pas le profil attendu, vérifiez d'abord qu'elle utilise le bon format et que vous avez fourni les bonnes valeurs.

- Avez-vous commencé avec la bonne URL (`findings` ou `entities`) ?
- Avez-vous spécifié le bon espace de noms ?
- Avez-vous fourni le bon identifiant ?

Si les valeurs sont correctes, vous pouvez également vérifier les points suivants.

- Le résultat ou l'entité appartient-il à un compte membre activé dans votre graphe de comportement ? Si le compte associé n'a pas été invité au graphe de comportement en tant que compte membre, le graphe de comportement ne contient aucune donnée pour ce compte.

  Si le compte d'un membre invité n'a pas accepté l'invitation, le graphe de comportement ne contient aucune donnée pour ce compte.

- Dans le cas d'un résultat, celui-ci est-il archivé ? Detective ne reçoit pas les résultats archivés d'Amazon GuardDuty.
- Le résultat ou l'entité s'est-il produit avant que Detective ne commence à ingérer des données dans votre graphe de comportement ? Si le résultat ou l'entité ne figure pas dans les données ingérées par Detective, le graphe de comportement ne contient aucune donnée correspondante.
- Le résultat ou l'entité provient-il de la bonne région ? Chaque graphe de comportement est spécifique à une région. Un graphe de comportement ne contient pas de données provenant d'autres régions.

Ajout d'URL Detective pour les résultats dans Splunk

Le projet Splunk Trumpet vous permet d'envoyer des données depuis les AWS services vers Splunk.

Vous pouvez configurer le projet Trumpet pour générer des URL Detective pour les résultats d'Amazon GuardDuty . Vous pouvez ensuite utiliser ces URL pour passer directement de Splunk aux profils de résultats Detective correspondants.

Le projet Trumpet est disponible sur GitHub https://github.com/splunk/ splunk-aws-project-trumpet.

Sur la page de configuration du projet Trumpet, dans AWS CloudWatch Events, sélectionnez Detective GuardDuty URLs.

Pivotement d'un volet de profil vers une autre console

Pour les EC2 instances, IAM les utilisateurs et IAM les rôles, vous pouvez naviguer directement depuis le panneau de profil détaillé vers la console correspondante. Les informations disponibles depuis la console peuvent fournir des informations supplémentaires pour votre enquête de sécurité.

Dans le EC2 panneau de profil des détails de l'EC2instance, l'identifiant de l'instance est lié à la EC2 console Amazon.

Dans le panneau de profil des détails de l'utilisateur, le nom d'utilisateur est lié à la IAM console.

Dans le panneau de profil des détails du rôle, le nom du rôle est lié à la IAM console.

Basculement d'un volet de profil vers un autre profil d'entité

Lorsqu'un volet de profil contient l'identifiant d'une entité différente, il s'agit généralement d'un lien vers le profil de cette entité. Les exceptions sont les liens vers Amazon EC2 et les IAM consoles

sur les profils d'EC2instance, d'IAMutilisateurs et de IAM rôles. Consultez the section called "Basculement vers une autre console".

Par exemple, à partir d'une liste d'adresses IP, vous pouvez peut-être afficher le profil d'une adresse IP spécifique. Ainsi, vous pourrez voir si d'autres informations sont disponibles pour vous aider à mener à bien votre enquête.

Exploration des détails d'activité sur un volet de profil

Au cours d'une enquête, vous souhaiterez peut-être approfondir le schéma d'activité d'une entité.

Dans les volets de profil suivants, vous pouvez afficher un résumé des détails de l'activité :

- Volume API d'appels global, à l'exception du panneau de profil sur le profil de l'agent utilisateur
- Géolocalisations nouvellement observées
- Volume VPC de débit global
- VPCvolume de flux vers et depuis l'adresse IP de recherche, pour les résultats associés à une adresse IP unique
- Détails du conteneur
- VPCvolume de flux pour les clusters
- Activité globale de Kubernetes API

Les détails de l'activité peuvent répondre aux types de questions suivants :

- Quelles adresses IP ont été utilisées ?
- Où se trouvaient ces adresses IP ?
- Quels API appels ont été effectués par chaque adresse IP, et à partir de quels services les a-t-elle effectués ?
- Quels principes ou identifiants de clé d'accès (AKIDs) ont été utilisés pour passer les appels ?
- Quelles ressources ont été utilisées pour passer ces appels ?
- Combien d'appels ont été passés ? Combien ont abouti et ont échoué ?
- Quel volume de données du journal de VPC flux a été envoyé vers ou depuis chaque adresse IP ?
- Quels conteneurs étaient actifs pour un cluster, une image ou un pod spécifique ?

Rubriques

- Détails de l'activité pour le volume global API d'appels
- Détails de l'activité pour une géolocalisation
- Détails de l'activité pour le volume VPC de débit global
- Activité globale de Kubernetes impliquant un cluster API EKS

Détails de l'activité pour le volume global API d'appels

Les détails de l'activité pour le volume global API des API appels indiquent les appels émis pendant une période sélectionnée.

Pour afficher les détails de l'activité pour un seul intervalle de temps, choisissez l'intervalle de temps sur le graphique.

Pour afficher les détails de l'activité pour la durée de validité actuelle, choisissez Afficher les détails pour la durée de validité.

Notez que Detective a commencé à enregistrer et à afficher le nom du service pour les API appels à partir du 14 juillet 2021. Cette date est mise en évidence sur la chronologie du volet de profil. Pour les activités effectuées avant cette date, le nom du service est Service inconnu.

Contenu des détails de l'activité (utilisateurs, rôles, comptes, sessions de rôles, EC2 instances, compartiments S3)

Pour IAM les utilisateurs, les IAM rôles, les comptes, les sessions de rôle, EC2 les instances et les compartiments S3, les détails de l'activité contiennent les informations suivantes :

- Chaque onglet fournit des informations sur l'ensemble des API appels émis pendant la période sélectionnée.

  Pour les compartiments S3, les informations reflètent API les appels effectués vers le compartiment S3.

  Les API appels sont regroupés en fonction des services qui les ont appelés. Pour les compartiments S3, le service est toujours Amazon S3. Si Detective ne parvient pas à déterminer le service à l'origine de l'appel, celui-ci est répertorié sous Service inconnu.
- Pour chaque entrée, les détails de l'activité indiquent le nombre d'appels réussis et échoués. L'onglet Adresses IP observées indique également l'emplacement de chaque adresse IP.

- Chaque entrée contient des informations sur les personnes qui ont passé les appels. Pour les comptes, les détails de l'activité identifient les utilisateurs ou les rôles. Pour les rôles, les détails de l'activité identifient les sessions de rôles. Pour les utilisateurs et les sessions de rôle, les détails de l'activité identifient les identifiants de clé d'accès (AKIDs).

  Notez qu'à compter du 14 juillet 2021, pour les profils de compte, les détails de l'activité indiquent les utilisateurs ou les rôles au lieu deAKIDs. Pour les profils de rôle, les détails de l'activité indiquent les sessions de rôle au lieu deAKIDs. Pour les activités qui ont lieu avant le 14 juillet 2021, l'appelant est répertorié comme ressource inconnue.

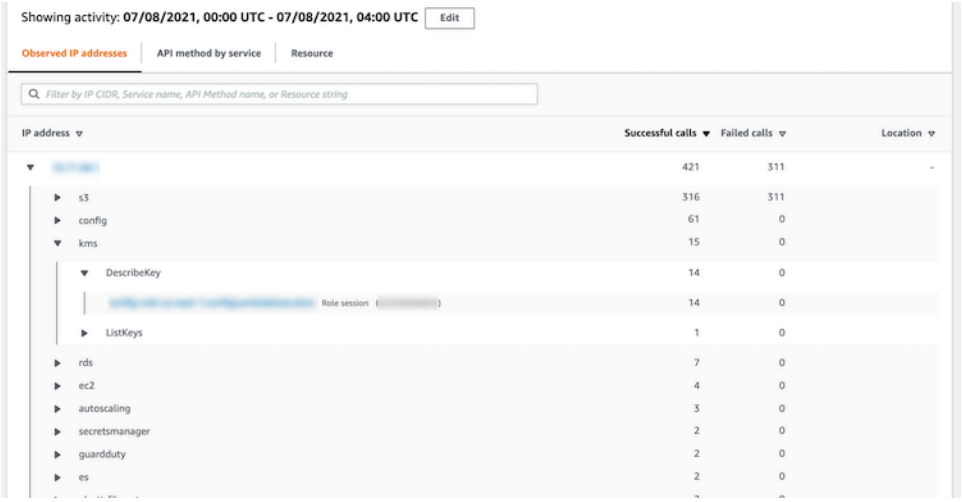
Les détails de l'activité contiennent les onglets suivants :

Adresses IP observées

Affiche initialement la liste des adresses IP utilisées pour émettre API des appels.

Vous pouvez développer chaque adresse IP pour afficher la liste des API appels émis à partir de cette adresse IP. Les API appels sont regroupés en fonction des services qui les ont appelés. Pour les compartiments S3, le service est toujours Amazon S3. Si Detective ne parvient pas à déterminer le service à l'origine de l'appel, celui-ci est répertorié sous Service inconnu.

Vous pouvez ensuite développer chaque API appel pour afficher la liste des appelants provenant de cette adresse IP. Selon le profil, l'appelant peut être un utilisateur, un rôle, une session de rôle ouAKID.



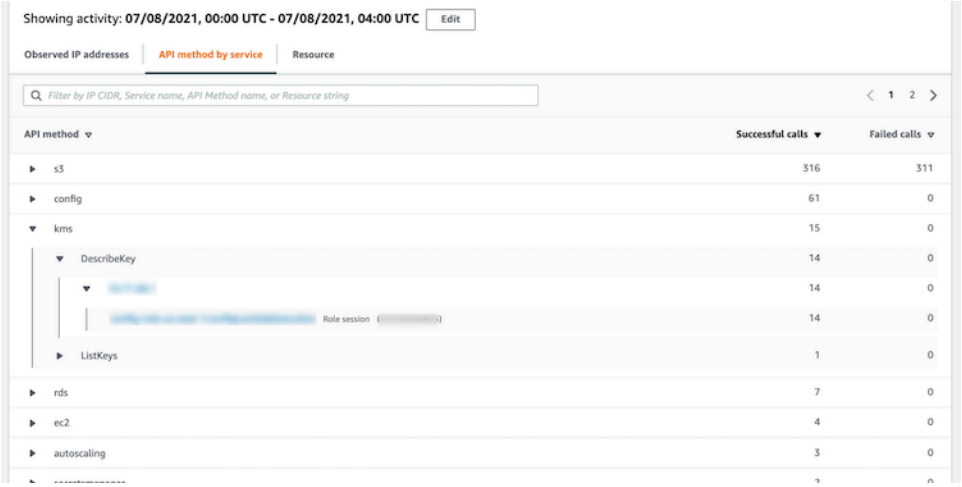
APIméthode par service

Affiche initialement la liste des API appels émis. Les API appels sont regroupés en fonction des services qui les ont émis. Pour les compartiments S3, le service est toujours Amazon S3. Si

Detective ne parvient pas à déterminer le service à l'origine de l'appel, celui-ci est répertorié sous Service inconnu.

Vous pouvez développer chaque API méthode pour afficher la liste des adresses IP à partir desquelles les appels ont été émis.

Vous pouvez ensuite développer chaque adresse IP pour afficher la liste de l'AKIDsAPIappel émis à partir de cette adresse IP.

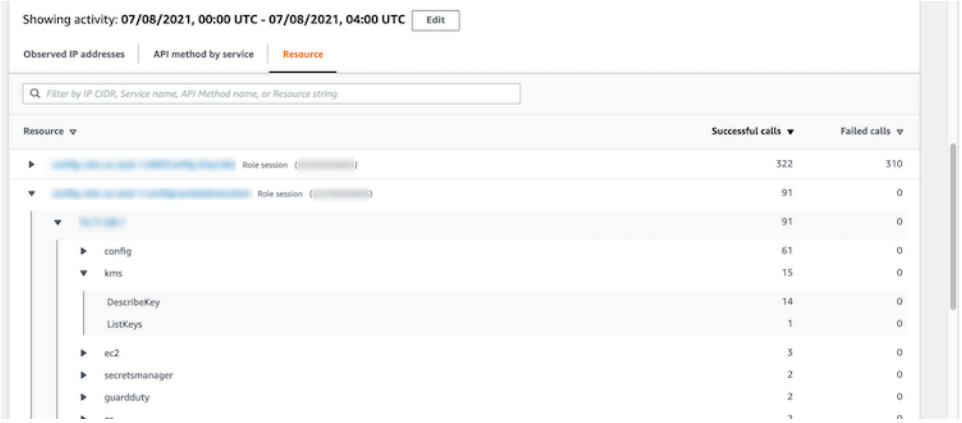


ID de ressource ou de clé d'accès

Affiche initialement la liste des utilisateurs, des rôles, des sessions de rôle ou AKIDs qui ont été utilisés pour émettre API des appels.

Vous pouvez développer chaque appelant pour afficher la liste des adresses IP à partir desquelles il a émis API des appels.

Vous pouvez ensuite développer chaque adresse IP pour afficher la liste des API appels émis à partir de cette adresse IP par cet appelant. Les API appels sont regroupés en fonction des services qui les ont émis. Pour les compartiments S3, le service est toujours Amazon S3. Si Detective ne parvient pas à déterminer le service à l'origine de l'appel, celui-ci est répertorié sous Service inconnu.



Contenu des détails de l'activité (adresses IP)

Pour les adresses IP, les détails de l'activité contiennent les informations suivantes :

- Chaque onglet fournit des informations sur l'ensemble des API appels émis pendant la période sélectionnée. Les API appels sont regroupés en fonction des services qui les ont émis. Si Detective ne parvient pas à déterminer le service à l'origine de l'appel, celui-ci est répertorié sous Service inconnu.
- Pour chaque entrée, les détails de l'activité indiquent le nombre d'appels réussis et échoués.

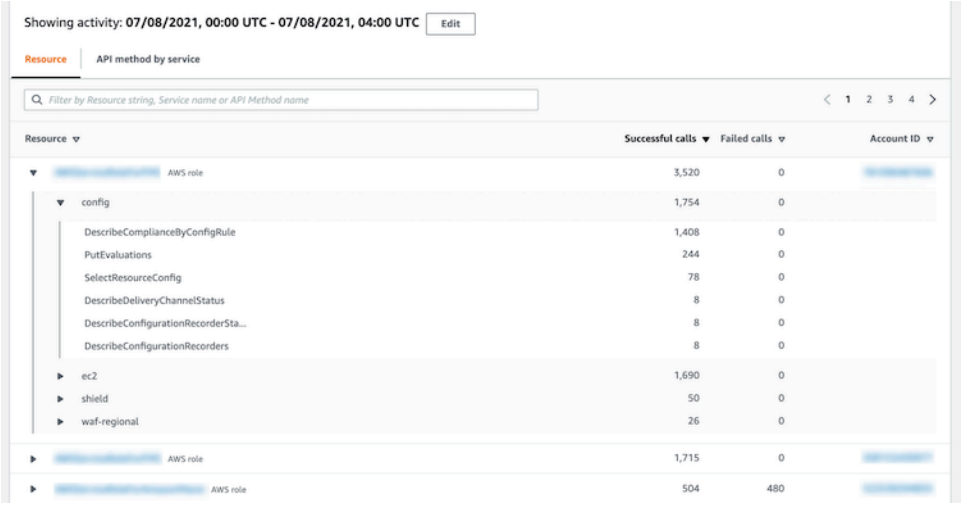
Les détails de l'activité contiennent les onglets suivants :

Ressource

Affiche initialement la liste des ressources qui ont émis API des appels depuis l'adresse IP.

Pour chaque ressource, la liste inclut le nom, le type et le compte AWS de la ressource.

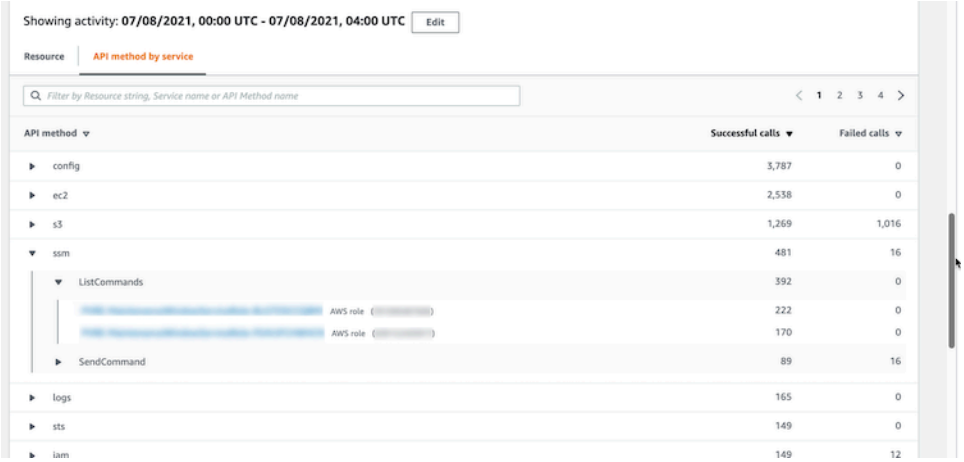
Vous pouvez développer chaque ressource pour afficher la liste des API appels émis par la ressource à partir de l'adresse IP. Les API appels sont regroupés en fonction des services qui les ont émis. Si Detective ne parvient pas à déterminer le service à l'origine de l'appel, celui-ci est répertorié sous Service inconnu.



APIméthode par service

Affiche initialement la liste des API appels émis. Les API appels sont regroupés en fonction des services qui les ont émis. Si Detective ne parvient pas à déterminer le service à l'origine de l'appel, celui-ci est répertorié sous Service inconnu.

Vous pouvez développer chaque API appel pour afficher la liste des ressources qui ont émis l'APIappel à partir de l'adresse IP pendant la période sélectionnée.



Tri des détails de l'activité

Vous pouvez trier les détails de l'activité selon l'une des colonnes de la liste.

Lorsque vous effectuez un tri à l'aide de la première colonne, seule la liste de niveau supérieur est triée. Les listes de niveau inférieur sont toujours triées en fonction du nombre d'APIappels réussis.

Filtrer les détails de l'activité

Vous pouvez utiliser les options de filtrage pour vous concentrer sur des sous-ensembles ou des aspects spécifiques de l'activité représentés dans les détails de l'activité.

Dans tous les onglets, vous pouvez filtrer la liste en fonction de l'une des valeurs de la première colonne.

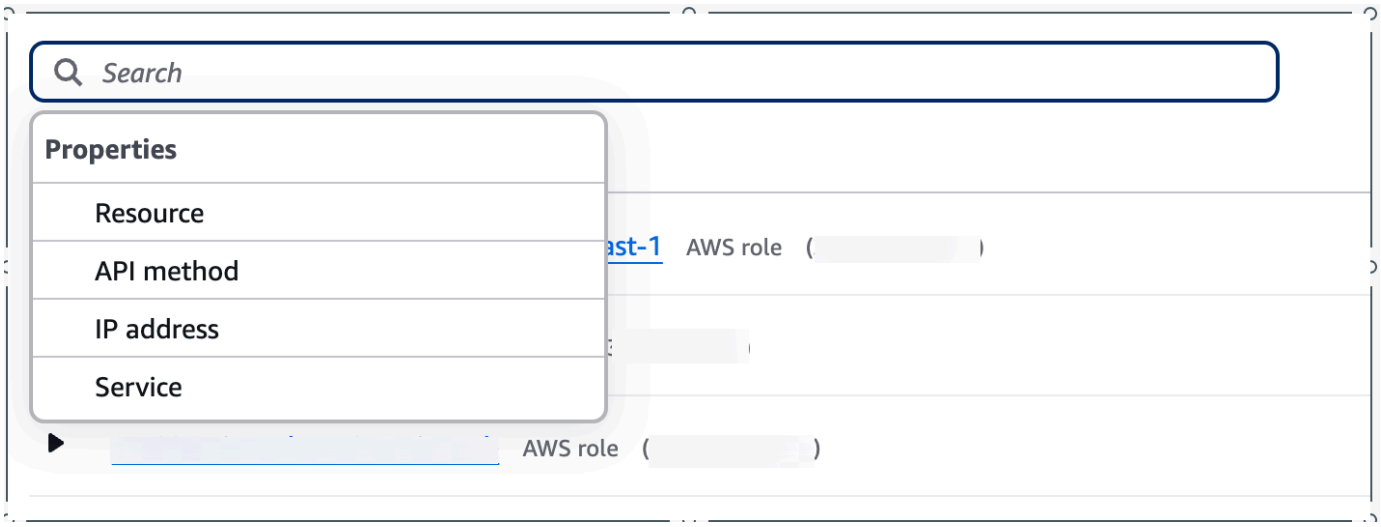
Pour ajouter un filtre

1. Choisissez la zone de filtre.
2. Dans Propriétés, choisissez la propriété à utiliser pour le filtrage.
3. Indiquez la valeur à utiliser pour le filtrage. Le filtre prend en charge les valeurs partielles. Par exemple, lorsque vous filtrez par API méthode, si vous filtrez par**`Instance`**, les résultats incluent toute API opération dont le nom `Instance` figure dans son nom. Par conséquent, `ListInstanceAssociations` et `UpdateInstanceInformation` correspondraient tous deux.

   Pour les noms de service, les API méthodes et les adresses IP, vous pouvez spécifier une valeur ou choisir un filtre intégré.

   Pour les API sous-chaînes communes, choisissez la sous-chaîne qui représente le type d'opération, telle que `ListCreate`, ou. `Delete` Le nom de chaque API méthode commence par le type d'opération.

   Pour CIDRles modèles, vous pouvez choisir d'inclure uniquement les adresses IP publiques, les adresses IP privées ou les adresses IP correspondant à un CIDR modèle spécifique.
4. Choisissez une option booléenne ***`Resource`*** ou ***`Service`*** : Contient ou ! : Ne contient pas ; ou *`API method`* ou *`IP address`* = Est égal à ou ! : N'équivaut pas à définir des filtres.



Pour supprimer une balise, choisissez le x situé dans l'angle supérieur droit de la balise.

Pour effacer tous les filtres, choisissez Supprimer le filtre.

Sélection de la plage de temps pour les détails de l'activité

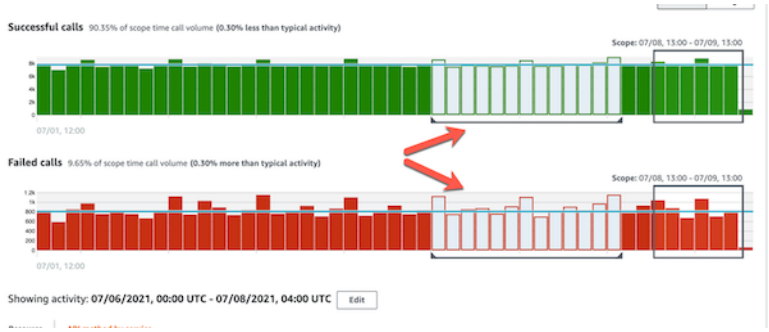
Lorsque vous affichez les détails de l'activité pour la première fois, la plage de temps correspond soit à la durée de validité, soit à un intervalle de temps sélectionné. Vous pouvez modifier la plage horaire pour les détails de l'activité.

Pour modifier la plage de temps pour les détails de l'activité

1. Choisissez Modifier.
2. Dans la fenêtre de modification de l'heure, choisissez l'heure de début et de fin à utiliser.

   Pour définir la fenêtre temporelle sur la durée de validité par défaut du profil, choisissez Définir sur la durée de validité par défaut.
3. Choisissez Mettre à jour la période.

La plage de temps pour les détails de l'activité est mise en évidence sur les graphiques du volet de profil.



Interrogation des journaux bruts

Amazon Detective est intégré à Amazon Security Lake, ce qui signifie que vous pouvez interroger et récupérer les données brutes des journaux stockées par Security Lake. Pour plus de détails sur cette intégration, consultez Detective Integration avec Security Lake.

Grâce à cette intégration, vous pouvez collecter et interroger des journaux et des événements provenant des sources suivantes, prises en charge de manière native par Security Lake.

- AWS CloudTrail événements de gestion version 1.0 et versions ultérieures
- Amazon Virtual Private Cloud (AmazonVPC) Flow Logs version 1.0 et ultérieure
- Journal d'audit Amazon Elastic Kubernetes Service (EKSAmazon) version 2.0

> **Note**
>
> L'interrogation des journaux de données brutes dans Detective n'entraîne pas de frais supplémentaires. Les frais d'utilisation des autres AWS services, y compris Amazon Athena, s'appliquent toujours aux tarifs publiés.

Pour interroger des journaux bruts

1. Choisissez les détails d'affichage pour la durée de validité.
2. À partir de là, vous pouvez commencer à interroger les journaux bruts.
3. Dans le tableau d'aperçu des journaux bruts, vous pouvez consulter les journaux et les événements extraits en interrogeant les données de Security Lake. Pour plus de détails sur les journaux d'événements bruts, vous pouvez consulter les données affichées dans Amazon Athena.

Dans le tableau d'interrogation des journaux bruts, vous pouvez annuler la demande de requête, afficher les résultats dans Amazon Athena et télécharger les résultats sous la forme d'un fichier de valeurs séparées par des virgules (.csv).

Si vous voyez des journaux dans Detective, mais que la requête n'a renvoyé aucun résultat, les raisons peuvent en être les suivantes.

- Les journaux bruts peuvent être disponibles dans Detective avant d'apparaître dans les tableaux des journaux de Security Lake. Réessayez ultérieurement.
- Les journaux peuvent ne pas être présents dans Security Lake. Si vous avez attendu pendant une longue période, cela indique que les journaux sont absents de Security Lake. Contactez votre administrateur Security Lake pour résoudre le problème.

Détails de l'activité pour une géolocalisation

Les détails de l'activité pour les nouvelles géolocalisations observées indiquent les API appels émis à partir d'une géolocalisation pendant la période couverte par le champ d'application. Les API appels incluent tous les appels émis depuis la géolocalisation. Ils ne se limitent pas aux appels utilisant l'entité de résultat ou de profil. Pour les compartiments S3, les appels d'activité sont des API appels effectués vers le compartiment S3.

Detective détermine l'emplacement des demandes à l'aide des bases de MaxMind données GeoIP. MaxMind fait état d'une très grande précision de ses données au niveau des pays, bien que la précision varie en fonction de facteurs tels que le pays et le type de propriété intellectuelle. Pour plus d'informations MaxMind, consultez la section Géolocalisation MaxMind IP. Si vous pensez que l'une des données GeoIP est incorrecte, vous pouvez envoyer une demande de correction à Maxmind à l'adresse MaxMind Correct Geo Data. IP2

Les API appels sont regroupés en fonction des services qui les ont émis. Pour les compartiments S3, le service est toujours Amazon S3. Si Detective ne parvient pas à déterminer le service à l'origine de l'appel, celui-ci est répertorié sous Service inconnu.

Pour afficher les détails de l'activité, effectuez l'une des actions suivantes :

- Sur la carte, choisissez une géolocalisation.
- Dans la liste, choisissez Détails pour une géolocalisation.

Les détails de l’activité remplacent la liste de géolocalisation. Pour revenir à la liste de géolocalisation, choisissez Retour à tous les résultats.

Notez que Detective a commencé à enregistrer et à afficher le nom du service pour les API appels à partir du 14 juillet 2021. Pour les activités effectuées avant cette date, le nom du service est Service inconnu.

Détails du contenu de l’activité

Chaque onglet fournit des informations sur tous les API appels émis depuis la géolocalisation pendant la période couverte par le champ d'application.

Pour chaque adresse IP, ressource et API méthode, la liste indique le nombre d'APIappels réussis et échoués.

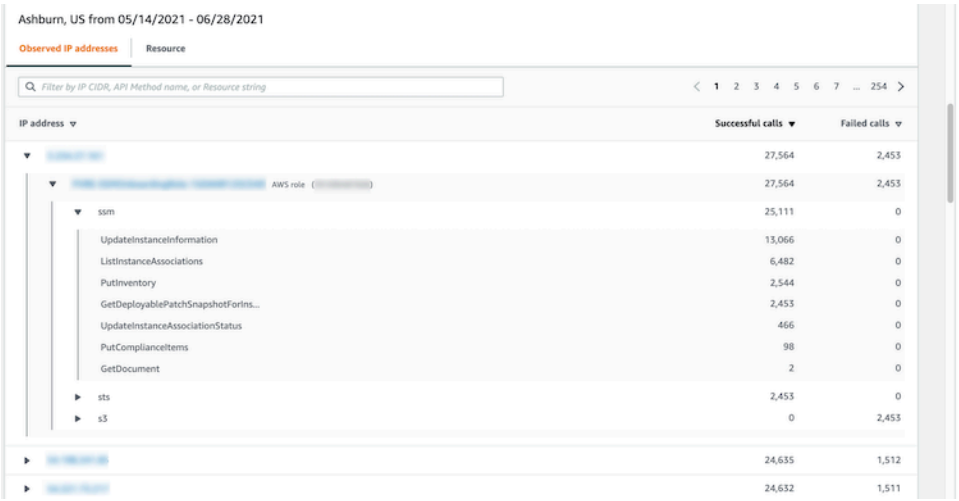
Les détails de l’activité contiennent les onglets suivants :

Adresses IP observées

Affiche initialement la liste des adresses IP utilisées pour émettre des API appels à partir de la géolocalisation sélectionnée.

Vous pouvez développer chaque adresse IP pour afficher les ressources qui ont émis des API appels à partir de cette adresse IP. La liste affiche le nom de la ressource. Pour voir l’ID principal, passez le curseur sur le nom.

Vous pouvez ensuite développer chaque ressource pour afficher les API appels spécifiques émis par cette ressource à partir de cette adresse IP. Les API appels sont regroupés en fonction des services qui les ont émis. Pour les compartiments S3, le service est toujours Amazon S3. Si Detective ne parvient pas à déterminer le service à l’origine de l’appel, celui-ci est répertorié sous Service inconnu.

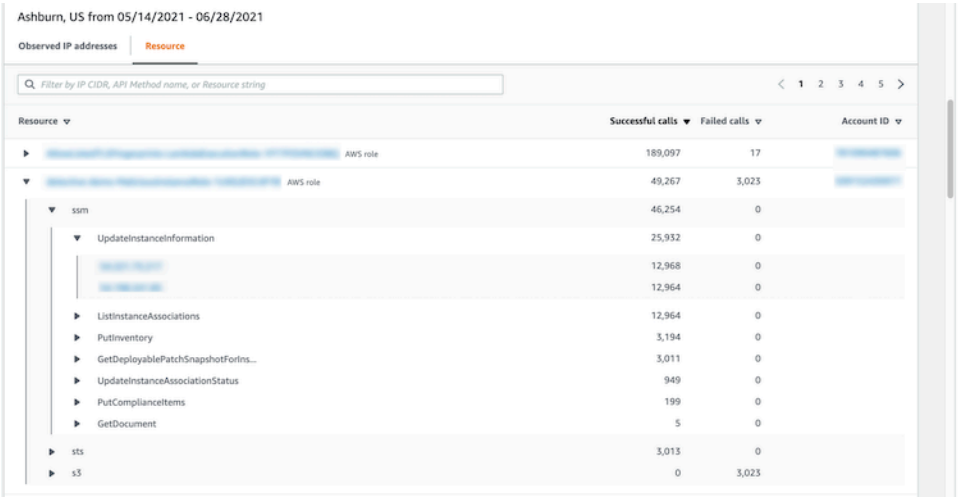


Ressource

Affiche initialement la liste des ressources qui ont émis des API appels depuis la géolocalisation sélectionnée. La liste affiche le nom de la ressource. Pour voir l'identifiant principal, faites une pause sur le nom. Pour chaque ressource, l'onglet Ressource affiche également les Compte AWS associés.

Vous pouvez développer chaque utilisateur ou rôle pour afficher la liste des API appels émis par cette ressource. Les API appels sont regroupés en fonction des services qui les ont émis. Pour les compartiments S3, le service est toujours Amazon S3. Si Detective ne parvient pas à déterminer le service à l'origine de l'appel, celui-ci est répertorié sous Service inconnu.

Vous pouvez ensuite développer chaque API appel pour afficher la liste des adresses IP à partir desquelles la ressource a émis l'APIappel.



Tri des détails de l’activité

Vous pouvez trier les détails de l’activité selon l’une des colonnes de la liste.

Lorsque vous effectuez un tri à l’aide de la première colonne, seule la liste de niveau supérieur est triée. Les listes de niveau inférieur sont toujours triées en fonction du nombre d'APIappels réussis.

Filtrer les détails de l’activité

Vous pouvez utiliser les options de filtrage pour vous concentrer sur des sous-ensembles ou des aspects spécifiques de l’activité représentés dans les détails de l’activité.

Dans tous les onglets, vous pouvez filtrer la liste en fonction de l’une des valeurs de la première colonne.

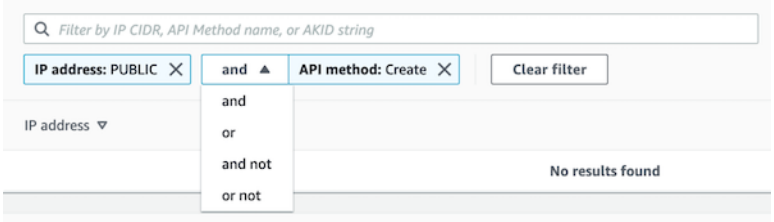
Pour ajouter un filtre

1. Choisissez la zone de filtre.
2. Dans Propriétés, choisissez la propriété à utiliser pour le filtrage.
3. Indiquez la valeur à utiliser pour le filtrage. Le filtre prend en charge les valeurs partielles. Par exemple, lorsque vous filtrez par API méthode, si vous filtrez par**`Instance`**, les résultats incluent toute API opération dont le nom `Instance` figure dans son nom. Par conséquent, `ListInstanceAssociations` et `UpdateInstanceInformation` correspondraient tous deux.

   Pour les noms de service, les API méthodes et les adresses IP, vous pouvez spécifier une valeur ou choisir un filtre intégré.

   Pour les API sous-chaînes communes, choisissez la sous-chaîne qui représente le type d'opération, telle que `ListCreate`, ou. `Delete` Le nom de chaque API méthode commence par le type d'opération.

   Pour CIDRles modèles, vous pouvez choisir d'inclure uniquement les adresses IP publiques, les adresses IP privées ou les adresses IP correspondant à un CIDR modèle spécifique.
4. Si vous disposez de plusieurs filtres, choisissez une option booléenne pour définir la manière dont ils sont connectés.



5. Pour supprimer une balise, choisissez le x situé dans l'angle supérieur droit de la balise.
6. Pour effacer tous les filtres, choisissez Supprimer le filtre.

Détails de l'activité pour le volume VPC de débit global

Pour une EC2 instance, les détails de l'activité pour le volume de VPC flux global indiquent les interactions entre l'EC2instance et les adresses IP pendant une période sélectionnée.

Pour un pod Kubernetes, le volume de VPCflux global affiche le volume global d'octets entrant et sortant de l'adresse IP attribuée au pod Kubernetes pour toutes les adresses IP de destination. L'adresse IP du pod Kubernetes n'est pas unique quand `hostNetwork:true`. Dans ce cas, le volet affiche le trafic vers d'autres pods ayant la même configuration et le nœud qui les héberge.

Pour une adresse IP, les détails de l'activité pour le volume de VPC flux global indiquent les interactions entre l'adresse IP et les EC2 instances au cours d'une plage de temps sélectionnée.

Pour afficher les détails de l'activité pour un seul intervalle de temps, choisissez l'intervalle de temps sur le graphique.

Pour afficher les détails de l'activité pour la durée de validité actuelle, choisissez Afficher les détails pour la durée de validité.

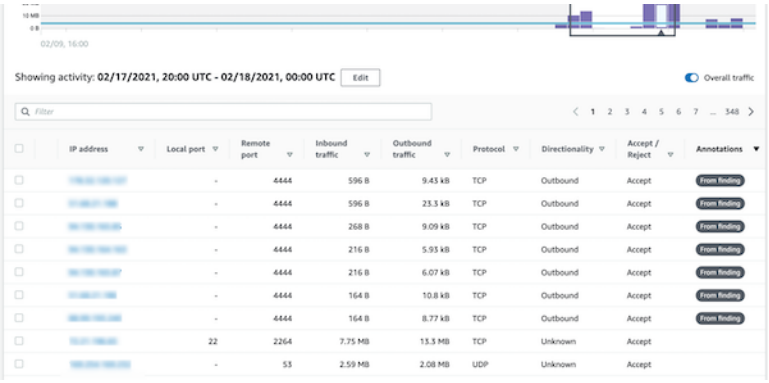
Détails du contenu de l'activité

Le contenu reflète l'activité au cours de la période sélectionnée.

EC2Par exemple, les détails de l'activité contiennent une entrée pour chaque combinaison unique d'adresse IP, de port local, de port distant, de protocole et de direction.

Pour une adresse IP, les détails de l'activité contiennent une entrée pour chaque combinaison unique d'EC2instance, de port local, de port distant, de protocole et de direction.

Chaque entrée indique le volume du trafic entrant, le volume du trafic sortant et indique si la demande d'accès a été acceptée ou rejetée. Sur les profils de résultats, la colonne Annotations indique à quel moment une adresse IP est liée au résultat en cours.



Tri des détails de l'activité

Vous pouvez trier les détails de l'activité selon l'une des colonnes du tableau.

Par défaut, les détails de l'activité sont d'abord triés en fonction des annotations, puis du trafic entrant.

Filtrer les détails de l'activité

Pour vous concentrer sur une activité spécifique, vous pouvez filtrer les détails de l'activité selon les valeurs suivantes :

- Adresse IP ou EC2 instance
- Port local ou distant
- Direction
- Protocole
- Si la demande a été acceptée ou rejetée

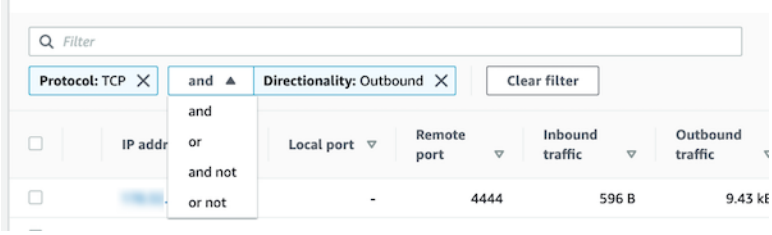
Pour ajouter et supprimer des filtres

1. Choisissez la zone de filtre.
2. Dans Propriétés, choisissez la propriété à utiliser pour le filtrage.
3. Indiquez la valeur à utiliser pour le filtrage. Le filtre prend en charge les valeurs partielles.

   Pour filtrer par adresse IP, vous pouvez soit spécifier une valeur, soit choisir un filtre intégré.

   Pour CIDRles modèles, vous pouvez choisir d'inclure uniquement les adresses IP publiques, les adresses IP privées ou les adresses IP correspondant à un CIDR modèle spécifique.

4. Si vous disposez de plusieurs filtres, choisissez une option booléenne pour définir la manière dont ils sont connectés.



5. Pour supprimer une balise, choisissez le x situé dans l'angle supérieur droit de la balise.
6. Pour effacer tous les filtres, choisissez Supprimer le filtre.

Sélection de la plage de temps pour les détails de l'activité

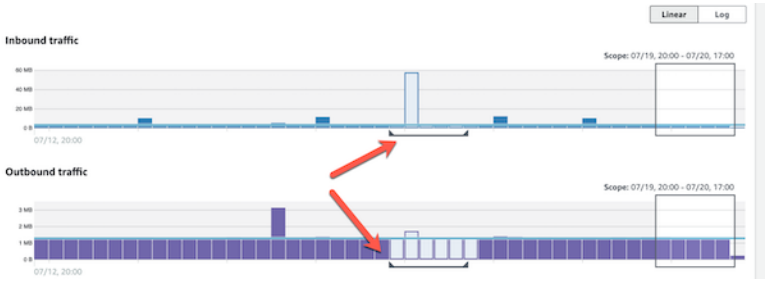
Lorsque vous affichez les détails de l'activité pour la première fois, la plage de temps correspond soit à la durée de validité, soit à un intervalle de temps sélectionné. Vous pouvez modifier la plage horaire pour les détails de l'activité.

Pour modifier la plage de temps pour les détails de l'activité

1. Choisissez Modifier.
2. Dans la fenêtre de modification de l'heure, choisissez l'heure de début et de fin à utiliser.

   Pour définir la fenêtre temporelle sur la durée de validité par défaut du profil, choisissez Définir sur la durée de validité par défaut.
3. Choisissez Mettre à jour la période.

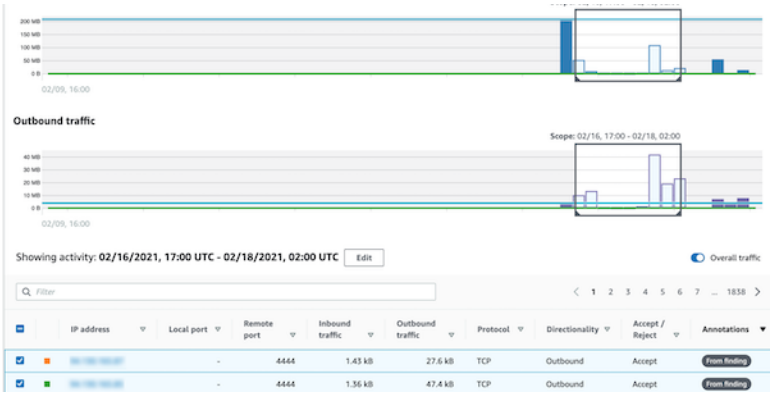
La plage de temps pour les détails de l'activité est mise en évidence sur les graphiques du volet de profil.



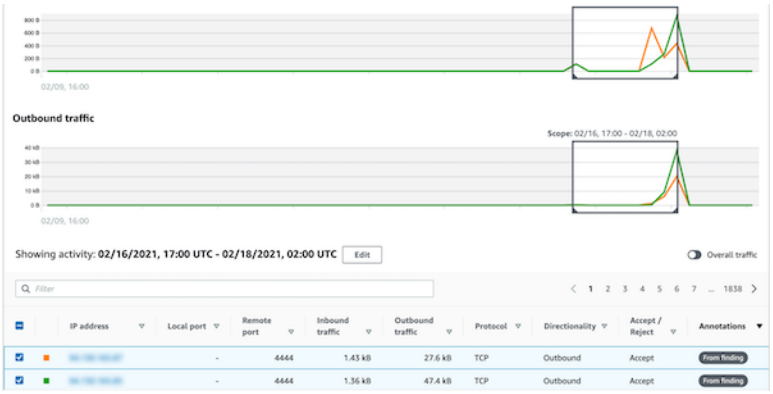
Affichage du volume de trafic pour les lignes sélectionnées

Lorsque vous identifiez les lignes qui présentent un intérêt, vous pouvez afficher dans les graphiques principaux le volume de trafic au fil du temps pour ces lignes.

Pour chaque ligne à ajouter aux graphiques, cochez la case correspondante. Pour chaque ligne sélectionnée, le volume est affiché sous forme de ligne sur les graphiques entrants ou sortants.



Pour vous concentrer sur le volume de trafic pour les entrées sélectionnées, vous pouvez masquer le volume global. Pour afficher ou masquer le volume de trafic global, activez l'option Trafic global.



Affichage du trafic VPC de flux pour les EKS clusters

Detective a une visibilité sur vos journaux de flux Amazon Virtual Private Cloud (AmazonVPC), qui représentent le trafic qui traverse vos clusters Amazon Elastic Kubernetes Service (Amazon). EKS Pour les ressources Kubernetes, le contenu des journaux de VPC flux dépend de l'interface réseau de conteneurs (CNI) déployée dans le cluster. EKS

Un EKS cluster avec une configuration par défaut utilise le VPC CNI plugin Amazon. Pour plus de détails, consultez Managing VPC CNI dans le guide de EKS l'utilisateur Amazon. Le VPC CNI plugin Amazon envoie le trafic interne avec l'adresse IP du pod et traduit l'adresse IP source en adresse IP

du nœud pour les communications externes. Detective peut capturer et corréler le trafic interne au pod approprié, mais il ne peut pas faire de même pour le trafic externe.

Si vous souhaitez que Detective ait une visibilité sur le trafic externe de vos pods, activez External Source Network Address Translation (SNAT). L'activation SNAT comporte des limites et des inconvénients. Pour plus de détails, consultez la section SNATconsacrée aux pods dans le guide de EKS l'utilisateur Amazon.

Si vous utilisez un autre CNI plugin, Detective a une visibilité limitée aux pods dotés de`hostNetwork:true`. Pour ces pods, le panneau VPCFlow affiche tout le trafic vers l'adresse IP du pod. Cela inclut le trafic vers le nœud hôte et tout pod du nœud contenant la configuration `hostNetwork:true`.

Detective affiche le trafic dans le panneau de VPCflux d'un EKS pod pour les configurations de EKS cluster suivantes :

- Dans un cluster doté du VPC CNI plugin Amazon, tout pod doté de la configuration `hostNetwork:false` envoie du trafic à l'intérieur VPC du cluster.
- Dans un cluster avec le VPC CNI plugin Amazon et la configuration`AWS_VPC_K8S_CNI_EXTERNALSNAT=`**`true`**, tout pod `hostNetwork:false` envoyant du trafic en dehors VPC du cluster.
- N'importe quel pod avec cette configuration `hostNetwork:true`. Le trafic provenant du nœud est mélangé au trafic provenant d'autres pods dotés de cette configuration `hostNetwork:true`.

Detective n'affiche pas le trafic dans le panneau de VPCflux pour :

- Dans un cluster doté du VPC CNI plugin Amazon et de la configuration`AWS_VPC_K8S_CNI_EXTERNALSNAT=false`, tout pod doté de la configuration `hostNetwork:false` envoie du trafic en dehors VPC du cluster.
- Dans un cluster sans le VPC CNI plug-in Amazon pour Kubernetes, n'importe quel pod avec la configuration. `hostNetwork:false`
- Tout pod envoyant le trafic vers un autre pod hébergé sur le même nœud.

Afficher le VPC flux de trafic pour Amazon partagé VPCs

Detective a accès à vos journaux de flux Amazon Virtual Private Cloud (AmazonVPC) à des fins de partage VPCs :

- Si un compte membre de Detective possède un compte Amazon partagé VPC et que d'autres comptes non Detective utilisent le partageVPC, Detective surveille tout le trafic provenant de celui-ci VPC et fournit une visualisation de l'ensemble du flux de trafic au sein duVPC.
- Si vous avez une EC2 instance Amazon dans un Amazon partagé VPC et que le VPC propriétaire du partage n'est pas membre de Detective, Detective ne surveillera aucun trafic provenant duVPC. Si vous souhaitez visualiser le flux de trafic au sein duVPC, vous devez ajouter le VPC propriétaire d'Amazon en tant que membre de votre Detective Graph.

Activité globale de Kubernetes impliquant un cluster API EKS

Les détails de l'activité globale de Kubernetes API impliquant un EKS cluster indiquent le nombre d'APIappels Kubernetes réussis et échoués émis pendant une période sélectionnée.

Pour afficher les détails de l'activité pour un seul intervalle de temps, choisissez l'intervalle de temps sur le graphique.

Pour afficher les détails de l'activité pour la durée de validité actuelle, choisissez Afficher les détails pour la durée de validité.

Contenu des détails de l'activité (cluster, pod, utilisateur, rôle, session de rôle)

Pour un cluster, un pod, un utilisateur, un rôle ou une session de rôle, les détails de l'activité contiennent les informations suivantes :

- Chaque onglet fournit des informations sur l'ensemble des API appels émis pendant la période sélectionnée.

  Pour les clusters, les API appels ont eu lieu à l'intérieur du cluster.

  Pour les pods, les API appels ciblaient le pod.

  Pour les utilisateurs, les rôles et les sessions de rôle, les API appels ont été émis par des utilisateurs Kubernetes qui se sont authentifiés en tant qu'utilisateur, rôle ou session de rôle.
- Pour chaque entrée, les détails de l'activité indiquent le nombre d'appels réussis, échoués, non autorisés et interdits.
- Les informations incluent l'adresse IP, le type d'appel Kubernetes, l'entité affectée par l'appel et le sujet (compte de service ou utilisateur) qui a effectué l'appel. À partir des détails de l'activité, vous pouvez accéder aux profils de l'adresse IP, du sujet et de l'entité concernée.

Les détails de l'activité contiennent les onglets suivants :

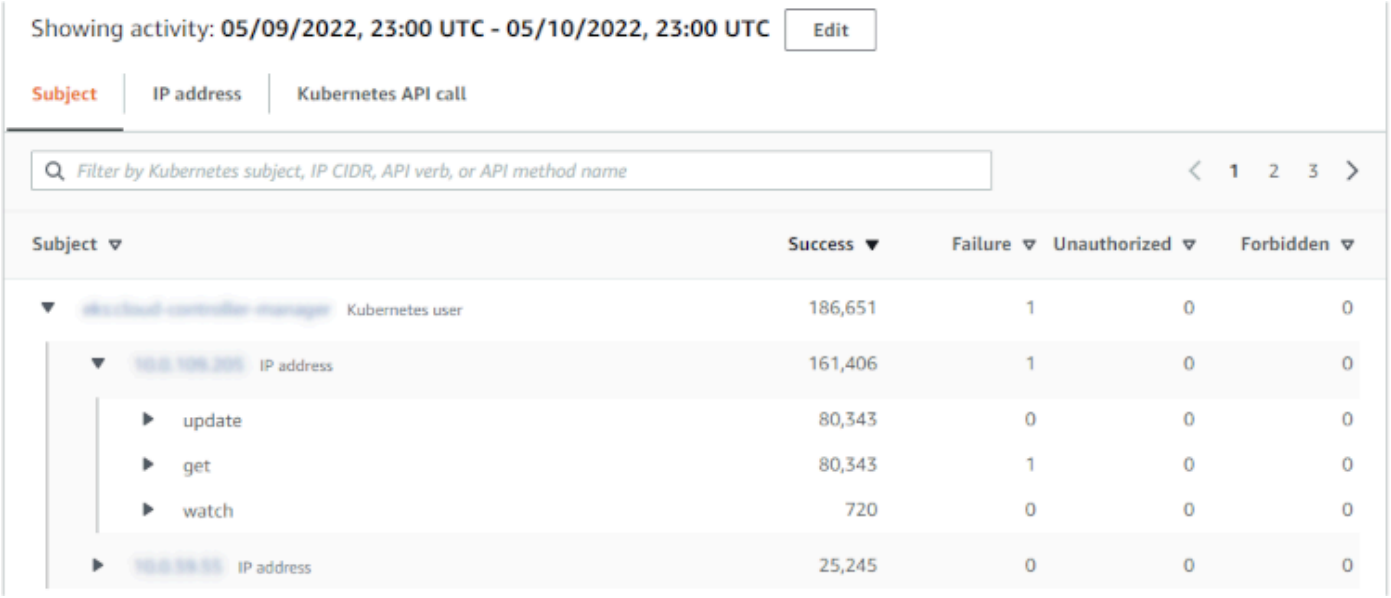
Sujet

Affiche initialement la liste des comptes de service et des utilisateurs utilisés pour passer des API appels.

Vous pouvez développer chaque compte de service et utilisateur pour afficher la liste des adresses IP à partir desquelles le compte ou l'utilisateur a passé API des appels.

Vous pouvez ensuite étendre chaque adresse IP pour afficher les API appels Kubernetes effectués par ce compte ou cet utilisateur à partir de cette adresse IP.

Développez l'APIappel Kubernetes pour voir le `requestURI` afin d'identifier l'action qui a été effectuée.



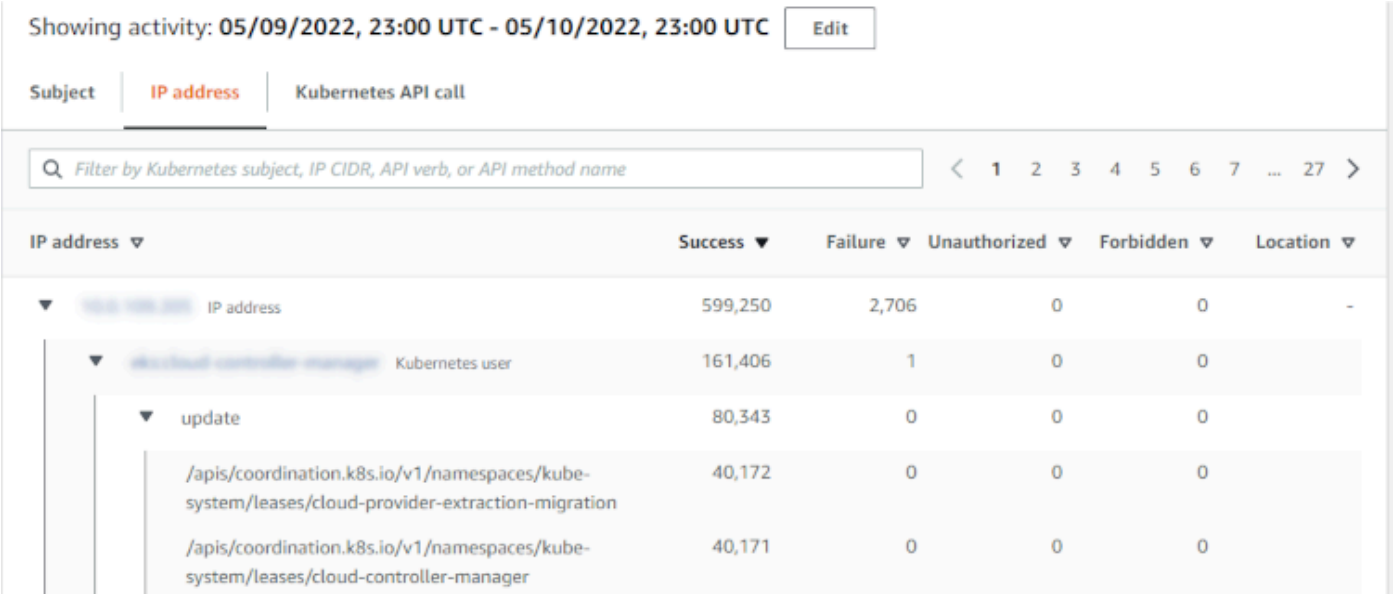
Adresse IP

Affiche initialement la liste des adresses IP à partir desquelles les API appels ont été effectués.

Vous pouvez développer chaque appel pour afficher la liste des sujets Kubernetes (comptes de service et utilisateurs) qui ont effectué l'appel.

Vous pouvez ensuite étendre chaque sujet à une liste des types d'APIappels effectués par le sujet pendant la durée du champ d'application.

Développez le type d'APIappel pour voir la demande URI d'identification de l'action effectuée.



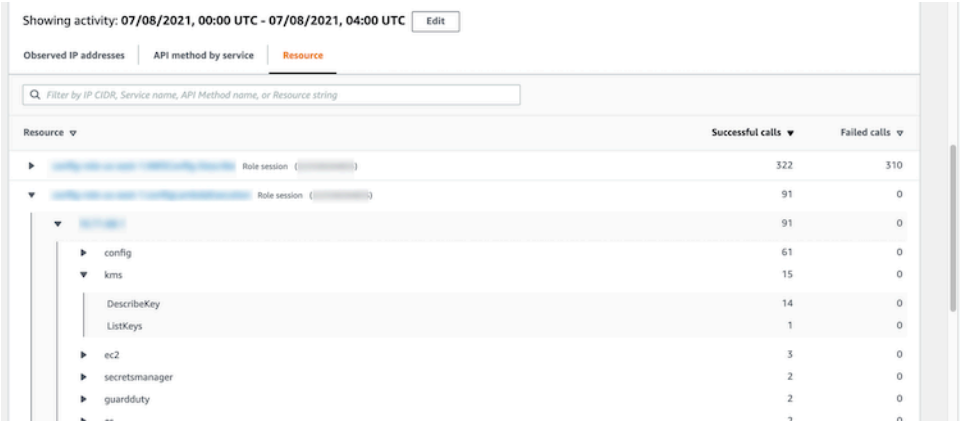
Appel Kubernetes API

Affiche initialement la liste des verbes d'appel Kubernetes. API

Vous pouvez développer chaque API verbe pour afficher le verbe requestURIs associé à cette action.

Vous pouvez ensuite développer chaque demande URI pour voir le sujet Kubernetes (comptes de service et utilisateurs) à l'origine de l'appel. API

Développez le sujet pour voir quel sujet IPs a été utilisé pour passer l'APIappel.



Tri des détails de l'activité

Vous pouvez trier les détails de l'activité selon l'une des colonnes de la liste.

Lorsque vous effectuez un tri à l'aide de la première colonne, seule la liste de niveau supérieur est triée. Les listes de niveau inférieur sont toujours triées en fonction du nombre d'APIappels réussis.

Filtrer les détails de l'activité

Vous pouvez utiliser les options de filtrage pour vous concentrer sur des sous-ensembles ou des aspects spécifiques de l'activité représentés dans les détails de l'activité.

Dans tous les onglets, vous pouvez filtrer la liste en fonction de l'une des valeurs de la première colonne.

Sélection de la plage de temps pour les détails de l'activité

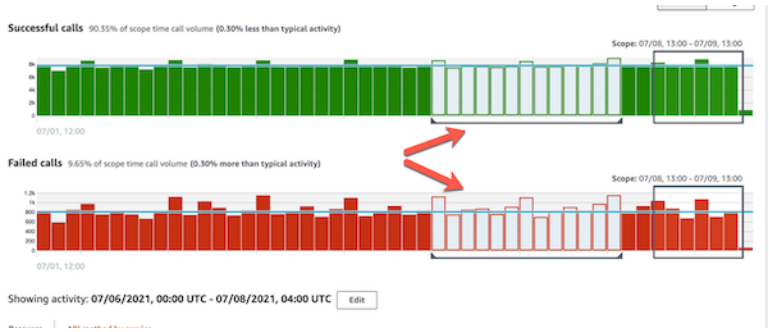
Lorsque vous affichez les détails de l'activité pour la première fois, la plage de temps correspond soit à la durée de validité, soit à un intervalle de temps sélectionné. Vous pouvez modifier la plage horaire pour les détails de l'activité.

Pour modifier la plage de temps pour les détails de l'activité

1. Choisissez Modifier.
2. Dans la fenêtre de modification de l'heure, choisissez l'heure de début et de fin à utiliser.

   Pour définir la fenêtre temporelle sur la durée de validité par défaut du profil, choisissez Définir sur la durée de validité par défaut.
3. Choisissez Mettre à jour la période.

La plage de temps pour les détails de l'activité est mise en évidence sur les graphiques du volet de profil.



Utilisation des instructions du volet de profil lors d'une enquête

Chaque volet de profil est conçu pour fournir des réponses à des questions spécifiques qui se posent lorsque vous menez une enquête et analysez l'activité des entités associées.

Les conseils fournis pour chaque volet de profil vous aident à trouver ces réponses.

Les instructions du volet de profil commencent par une seule phrase sur le volet lui-même. Ce guide fournit une brève explication des données présentées sur le volet.

Pour afficher des instructions plus détaillées pour un volet, choisissez Plus d'informations dans l'en-tête du volet. Ces instructions étendues apparaissent dans le volet d'aide.

Le guide peut fournir les types d'informations suivants :

- Vue d'ensemble du contenu du panel
- Comment utiliser le volet pour répondre aux questions pertinentes
- Prochaines étapes suggérées en fonction des réponses

Gestion de la durée de validité

Personnalisez la durée de validité utilisée pour limiter les données affichées sur les profils d'entité.

Les graphiques, les chronologies et les autres données affichées sur les profils d'entités sont tous basés sur la durée de validité actuelle du périmètre. La durée de validité est le résumé de l'activité d'une entité au fil du temps. Cela apparaît en haut à droite de chaque profil dans la console Amazon Detective. Les données affichées sur ces graphiques, chronologies et autres visualisations sont basées sur la durée de validité. Pour certains volets de profil, du temps supplémentaire est ajouté avant et après la durée de validité afin de fournir un contexte. Dans Detective, tous les horodatages sont affichés en UTC par défaut. Vous pouvez sélectionner votre fuseau horaire local en modifiant les préférences d'horodatage. Pour mettre à jour la préférence d'horodatage, voir the section called "Définition du format d'horodatage".

Detective Analytics utilise la durée de validité pour détecter toute activité inhabituelle. Le processus d'analyse enregistre l'activité pendant la durée de validité, puis la compare à l'activité pendant les 45 jours précédant la durée de validité. Il utilise également ce délai de 45 jours pour générer des bases d'activité.

Dans une vue d'ensemble des résultats, la durée de validité reflète la première et la dernière fois que le résultat a été observé. Pour plus d'informations sur la vue d'ensemble des résultats, consultez the section called "Vue d'ensemble des résultats".

Au fur et à mesure que vous menez une enquête, vous pouvez ajuster la durée de validité. Par exemple, si l'analyse initiale était basée sur l'activité d'une seule journée, vous souhaiterez peut-être étendre cette analyse à une semaine ou à un mois. La période prolongée pourrait vous aider à mieux comprendre si l'activité correspond à un schéma normal ou si elle est inhabituelle.

Vous pouvez également définir la durée de validité pour qu'elle corresponde à un résultat associé à l'entité actuelle.

Lorsque vous modifiez la durée de validité, Detective répète son analyse et met à jour les données affichées en fonction de la nouvelle durée de validité.

La durée de validité ne peut être inférieure à une heure ni supérieure à un an. Dates de début et de fin doivent être une heure après l'heure.

Définition de dates et d'heures de début et de fin spécifiques

Vous pouvez définir les dates de début et de fin de la durée de validité depuis la console Detective.

Pour définir des heures de début et de fin spécifiques pour la nouvelle durée de validité

1. Ouvrez la console Amazon à l'adresse https://console.aws.amazon.com/detective/.
2. Sur un profil d'entité, choisissez la durée de validité.
3. Dans le volet Modifier la durée de validité, sous Démarrer, choisissez les nouvelles date et heure de début de la durée de validité. Pour la nouvelle heure de début, vous choisissez uniquement l'heure.
4. Sous Fin, choisissez la nouvelle date et heure de fin pour la durée de validité. Pour la nouvelle heure de fin, vous choisissez uniquement l'heure. L'heure de fin doit être au moins une heure après l'heure de début.
5. Lorsque vous avez terminé les modifications, pour enregistrer les modifications et mettre à jour les données affichées, choisissez Mettre à jour la durée de validité.

Modifier la durée de validité

Lorsque vous définissez la durée de validité, Detective définit la durée de validité en fonction de cette durée par rapport à l'heure actuelle.

Pour modifier la durée de validité

1. Ouvrez la console Amazon à l'adresse https://console.aws.amazon.com/detective/.
2. Sur un profil d'entité, choisissez la durée de validité.
3. Dans le volet Modifier la durée de validité, à côté de Historique, choisissez la durée de validité.

   La spécification d'une plage horaire met à jour les paramètres de début et de fin.
4. Lorsque vous avez terminé les modifications, pour enregistrer les modifications et mettre à jour les données affichées, choisissez Mettre à jour la durée de validité.

Réglage de la durée de validité sur une fenêtre temporelle de résultats

Chaque résultat est associé à une fenêtre temporelle, qui reflète la première et la dernière fois que le résultat a été observé. Lorsque vous affichez une vue d'ensemble des résultats, la durée de validité passe à la fenêtre temporelle de résultats.

À partir d'un profil d'entité, vous pouvez aligner la durée de validité sur la fenêtre temporelle pour un résultat associé. Cela vous permet d'étudier l'activité qui s'est produite pendant cette période.

Pour aligner la durée de validité sur une fenêtre temporelle de résultats, dans le volet Résultats associés, choisissez le résultat que vous souhaitez utiliser.

Detective renseigne les détails des résultats et définit la durée de validité en fonction de la fenêtre temporelle de résultats.

Réglage de la durée de validité sur la page de résumé

Lorsque vous consultez la page Résumé, vous pouvez ajuster la durée de validité pour visualiser l'activité sur une période de 24 heures au cours des 365 jours précédents.

Pour définir la durée de validité sur la page Résumé

1. Ouvrez la console Amazon à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, choisissez Résumé.
3. Dans le volet Durée de validité, à côté de Résumé, vous pouvez modifier la date et l'heure de début. L'heure de début doit se situer dans les 365 derniers jours.

   Lorsque vous modifiez la date et l'heure de début, la date et l'heure de fin sont automatiquement mises à jour 24 heures après l'heure de début que vous avez choisie.

> **Note**
>
> Avec Detective, vous pouvez accéder à un an de données historiques sur les événements. Pour plus d'informations sur les données source dans Detective, voir Données source utilisées dans un graphe de comportement.

4. Lorsque vous avez terminé les modifications, pour enregistrer les modifications et mettre à jour les données affichées, choisissez Mettre à jour la durée de validité.

Afficher les détails des résultats associés dans Detective

Chaque profil d'entité contient un volet de résultats associé qui répertorie les résultats impliquant l'entité au cours de la durée de validité actuelle. L'implication d'une entité dans de multiples résultats indique qu'elle a été compromise. Les types de résultats peuvent également donner un aperçu du type d'activité présentant un souci.

Le volet des résultats associé est affiché juste en dessous du volet de profil des détails de l'entité.

Pour chaque résultat, le tableau comprend des informations sur les points suivants :

- Le titre du résultat, qui est également un lien vers la vue d'ensemble des résultats.
- Le AWS compte associé à la recherche, qui est également un lien vers le profil du compte
- Le type de résultats
- La première fois que le résultat a été observé
- La dernière fois que le résultat a été observé
- Le niveau de gravité du résultat

Pour afficher les détails d'un résultat, cliquez sur le bouton radio correspondant au résultat. Detective remplit le volet des détails des résultats situé à droite de la page. Detective modifie également la durée de validité pour qu'elle corresponde à la fenêtre temporelle de résultats. Cela vous permet de vous concentrer sur les activités qui se sont produites pendant cette période.

Si vous avez accédé au profil de l'entité à partir d'une vue d'ensemble des résultats, ce résultat est sélectionné automatiquement et les détails des résultats sont affichés.

Pour revenir à la vue d'ensemble des résultats à partir des détails des résultats, choisissez Voir toutes les entités associées.

Vous pouvez également archiver le résultat. Pour plus de détails, consultez Archivage d'une GuardDuty recherche Amazon.

Afficher les détails des entités à volume élevé dans Detective

Dans le graphe de comportement, Amazon Detective suit les relations entre les entités. Par exemple, chaque graphe de comportement suit le moment où un AWS utilisateur crée un AWS rôle et lorsqu'une EC2 instance se connecte à une adresse IP.

Lorsqu'une entité possède trop de relations au cours d'une période donnée, Detective ne peut pas enregistrer toutes les relations. Lorsque cela se produit pendant la durée de validité actuelle, Detective vous en informe. Detective fournit également une liste des occurrences d'entités à volume élevé.

Qu'est-ce qu'une entité à volume élevé ?

Pendant un intervalle de temps donné, une entité peut être la source ou la destination d'un très grand nombre de connexions. Par exemple, une EC2 instance peut avoir des connexions provenant de millions d'adresses IP.

Detective limite le nombre de connexions qu'il peut accepter pendant chaque intervalle de temps. Si une entité dépasse cette limite, Detective supprime les connexions pendant cet intervalle de temps.

Supposons, par exemple, que la limite soit de 100 000 000 connexions par intervalle de temps. Si une EC2 instance est connectée par plus de 100 000 000 d'adresses IP au cours d'un intervalle de temps, Detective supprime les connexions issues de cet intervalle de temps.

Toutefois, vous pouvez peut-être analyser cette activité en fonction de l'entité située à l'autre bout de la relation. Pour continuer l'exemple, alors qu'une EC2 instance peut être connectée à partir de millions d'adresses IP, une seule adresse IP se connecte à beaucoup moins d'EC2instances. Chaque profil d'adresse IP fournit des détails sur les EC2 instances auxquelles l'adresse IP est connectée.

Affichage de notification d'entité à volume élevé sur un profil

Detective affiche un avis en haut d'un résultat ou d'un profil d'entité si la durée de validité inclut un intervalle de temps pendant lequel l'entité présente un volume élevé. Pour les profils de résultats, l'avis est destiné à l'entité concernée.

L'avis comprend la liste des relations dont les intervalles de temps sont de volume élevé. Chaque entrée de liste contient une description de la relation et du début de l'intervalle de temps à volume élevé.

Un intervalle de temps à volume élevé peut être le signe d'une activité suspecte. Pour comprendre quelles autres activités se sont produites en même temps, vous pouvez concentrer votre enquête sur un intervalle de temps à volume élevé. L'avis relatif aux entités à volume élevé inclut une option permettant de définir la durée de validité en fonction de cet intervalle de temps.

Pour régler la durée de validité sur un intervalle de temps à volume élevé

1. Dans l'avis relatif aux entités à volume élevé, choisissez l'intervalle de temps.
2. Dans le menu contextuel, choisissez Appliquer la durée de validité.

Affichage de la liste des entités à volume élevé pour la durée de validité actuelle

La page Entités à volume élevé contient une liste des intervalles de temps et des entités à volume élevé pendant la durée de validité actuelle.

Pour afficher la page Entités à volume élevé

1. Ouvrez la console Amazon Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, sélectionnez Entités à volume élevé.

Chaque élément de la liste contient les informations suivantes :

- Le début de l'intervalle de temps à volume élevé
- L'identifiant et le type de l'entité
- Description de la relation, telle que « EC2 instance connectée depuis une adresse IP »

Vous pouvez filtrer et trier la liste par n'importe quelle colonne. Vous pouvez également accéder au profil d'entité d'une entité impliquée.

Pour accéder au profil d’une entité

1. Dans la liste des entités à volume élevé, choisissez la ligne à partir de laquelle vous souhaitez naviguer.
2. Choisissez Afficher le profil avec une durée de validité élevée.

Lorsque vous utilisez cette option pour accéder à un profil d’entité, la durée de validité est définie comme suit :

- La durée de validité commence 30 jours avant l’intervalle de temps à volume élevé.
- La durée de validité se termine à la fin de l’intervalle de temps à volume élevé.

Rechercher une découverte ou une entité dans Detective

Avec la fonction de recherche Amazon Detective, vous pouvez rechercher un résultat ou une entité. À partir des résultats de recherche, vous pouvez accéder à un profil d'entité ou à une vue d'ensemble des résultats. Si votre recherche renvoie plus de 10 000 résultats, seuls les 10 000 premiers résultats sont affichés. La modification de l'ordre de tri modifie les résultats renvoyés.

Vous pouvez exporter les résultats de votre recherche vers un fichier de valeurs séparées par des virgules (.csv). Ce fichier contient les données renvoyées dans la page de recherche. Les données sont exportées au format valeurs séparées par des virgules (CSV). Le nom de fichier des données exportées suit le modèle au format detective-page-panel-yyyy -mm-dd.csv. Vous pouvez enrichir vos enquêtes de sécurité en manipulant les données à l'aide d'autres AWS services, d'applications tierces ou de tableurs prenant en charge CSV l'importation.

> **Note**
>
> Si une exportation est en cours, attendez qu'elle soit terminée avant d'essayer d'exporter des données supplémentaires.

Finalisation de la recherche

Pour terminer la recherche, choisissez le type d'entité à rechercher. Fournissez ensuite l'identifiant exact ou l'identifiant avec des caractères génériques `*` ou `?`. Pour rechercher une plage d'adresses IP, vous pouvez également utiliser CIDR des notations par points. Consultez les exemples de chaînes de recherche suivants.

Pour les adresses IP :

- `1.0.*.*`
- `1.0.133.*`
- `1.0.0.0/16`
- `0.239.48.198/31`

Pour tous les autres types d'entités :

- `Admin`

- `ad*`
- `ad*n`
- `ad*n*`
- `adm?n`
- `a?m*`
- `*min`

Pour chaque type d'entité, les identifiants suivants sont pris en charge :

- Pour les résultats, l'identifiant de recherche ou le nom de la ressource Amazon (ARN).
- Pour les AWS comptes, l'identifiant du compte.
- Pour AWS les rôles et AWS les utilisateurs, soit l'ID principal, soit le nom, soit leARN.
- Pour les clusters de conteneurs, le nom du cluster ouARN.
- Pour les images du conteneur, le référentiel ou le résumé complet de l'image du conteneur.
- Pour les pods ou les tâches du conteneur, le nom UID du pod ou le pod.
- Pour les EC2 instances, l'identifiant de l'instance ou leARN.
- Pour le groupe de résultats, l'identifiant du groupe de résultats.
- Pour les adresses IP, l'adresse en notation CIDR ou en points.
- Pour les sujets Kubernetes (comptes de service ou utilisateurs), le nom.
- Pour une session de rôle, vous pouvez utiliser l'une des valeurs suivantes pour effectuer une recherche :
  - Identifiant de session de rôle.

    L'identifiant de la session du rôle utilise le format *<rolePrincipalID>*:*<sessionName>*.

    Voici un exemple : `AROA12345678910111213:MySession`.
  - Séance de rôle ARN
  - Nom de la session
  - ID principal du rôle assumé
  - Nom du rôle assumé
- Pour les compartiments S3, le nom du compartiment ou du compartimentARN.
- Pour les utilisateurs fédérés, l'ID principal ou le nom d'utilisateur. L'ID principal est *<identityProvider>*:*<username>* ou *<identityProvider>*:*<audience>*:*<username>*.

- Pour les agents utilisateurs, le nom de l'agent utilisateur.

Pour rechercher un résultat ou une entité

1. Connectez-vous au AWS Management Console. Ouvrez ensuite la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, sélectionnez Recherche.
3. Dans le menu Choisir un type, choisissez le type d'article que vous recherchez.

   Notez que lorsque vous sélectionnez Utilisateur, vous pouvez rechercher un AWS utilisateur ou un utilisateur fédéré.

   Les exemples tirés de vos données contiennent un ensemble d'exemples d'identifiants du type sélectionné qui figurent dans les données de votre graphe de comportement. Pour afficher le profil de l'un des exemples, choisissez son identifiant.
4. Entrez l'identifiant exact ou un identifiant avec des caractères génériques à rechercher.

   La recherche ne distingue pas les majuscules et minuscules.
5. Choisissez Rechercher ou appuyez sur Entrée.

Utilisation des résultats de recherche

Lorsque vous terminez la recherche, Detective affiche une liste contenant jusqu'à 10 000 résultats correspondants. Pour les recherches utilisant un identifiant unique, il n'y a qu'un seul résultat correspondant.

Dans les résultats, pour accéder au profil de l'entité ou à la vue d'ensemble des résultats, choisissez l'identifiant.

Pour les résultats, les rôles, les utilisateurs et EC2 les instances, les résultats de recherche incluent le compte associé. Pour accéder au profil du compte, choisissez l'identifiant du compte.

Résolution des problèmes liés à la recherche

Si Detective ne trouve pas le résultat ou l'entité, vérifiez d'abord que vous avez saisi le bon identifiant. Si l'identifiant est correct, vous pouvez également vérifier les points suivants.

- Le résultat ou l’entité appartient-il à un compte membre activé dans votre graphe de comportement ? Si le compte associé n’a pas été invité au graphe de comportement en tant que compte membre, le graphe de comportement ne contient aucune donnée pour ce compte.

  Si le compte d’un membre invité n’a pas accepté l’invitation, le graphe de comportement ne contient aucune donnée pour ce compte.
- Dans le cas d’un résultat, celui-ci est-il archivé ? Detective ne reçoit pas les résultats archivés d'Amazon GuardDuty.
- Le résultat ou l’entité s’est-il produit avant que Detective ne commence à ingérer des données dans votre graphe de comportement ? Si le résultat ou l’entité ne figure pas dans les données ingérées par Detective, le graphe de comportement ne contient aucune donnée correspondante.
- Le résultat ou l’entité provient-il de la bonne région ? Chaque graphe de comportement est spécifique à un Région AWS. Un graphe de comportement ne contient pas de données provenant d’autres régions.

Gestion des comptes dans Detective

Lorsqu'un compte active Detective, il devient le compte administrateur du graphe de comportement, et il choisit les comptes des membres pour le graphe de comportement. Un compte administrateur peut inviter des comptes à rejoindre un graphe de comportement. Lorsque le compte accepte l'invitation, Detective active le compte en tant que compte membre. Les comptes membres ajoutés sur invitation peuvent se supprimer du graphe de comportement.

Lorsqu'un compte est activé en tant que compte membre, Detective commence l'ingestion et l'extraction des données du compte membre dans ce graphe de comportement.

Chaque graphe de comportement contient les données d'un ou plusieurs comptes. Un graphe de comportement peut comporter jusqu'à 1 200 comptes membres.

Si vous êtes intégré à AWS Organizations, le compte de gestion de l'organisation désigne le compte administrateur Detective de l'organisation. Ce compte administrateur Detective devient alors le compte administrateur du graphe de comportement de l'organisation. Le compte administrateur Detective peut activer n'importe quel compte de l'organisation comme compte membre dans le graphe de comportement. Les comptes de l'organisation ne peuvent pas se dissocier du graphe de comportement.

Detective facture à chaque compte les données qu'il fournit à chaque graphe de comportement. Pour plus d'informations sur le suivi du volume de données pour chaque compte dans un graphique de comportement, consultez la section Prévision et surveillance des coûts d'Amazon Detective.

Table des matières

- Restrictions et recommandations relatives aux comptes dans Detective
- Utilisation des Organisations pour gérer les comptes de graphes comportementaux
- Désignation de l'administrateur Detective d'une organisation
- Actions disponibles pour les comptes
- Consulter la liste des comptes
- Gérer les comptes de l'organisation en tant que comptes membres de Detective
- Gérer les comptes des membres invités dans Detective
- Pour les comptes membres : gestion des invitations des graphes de comportement et des appartenances

- Effet des actions du compte sur les graphes de comportement
- Utilisation de scripts Detective Python pour gérer les comptes

Restrictions et recommandations relatives aux comptes dans Detective

Lorsque vous gérez des comptes dans Amazon Detective, tenez compte des restrictions et recommandations suivantes.

Nombre maximal de comptes membres

Detective autorise jusqu'à 1 200 comptes membres dans chaque graphe de comportement.

Si vous avez l' AWS Organizations habitude de gérer des comptes, Detective affiche par défaut jusqu'à 5 000 comptes membres sur la page de gestion des comptes. Si vous souhaitez afficher tous les comptes, sélectionnez Charger tous les comptes. L'affichage de tous les résultats peut prendre plusieurs minutes.

Comptes et régions

Si vous utilisez AWS Organizations pour gérer des comptes, le compte de gestion de l'organisation désigne un compte d'administrateur Detective pour l'organisation. Le compte administrateur Detective devient le compte administrateur Detective du graphe de comportement de l'organisation.

Le compte administrateur Detective doit être le même dans toutes les régions. Le compte de gestion de l'organisation désigne le compte administrateur Detective séparément dans chaque région. Le compte administrateur Detective gère également les graphes de comportement de l'organisation et les comptes des membres séparément dans chaque région.

Pour les comptes membres créés sur invitation, l'association administrateur-membre est créée uniquement dans la région d'où l'invitation est envoyée. Le compte administrateur doit activer Detective dans chaque région et dispose d'un graphe de comportement distinct dans chaque région. Le compte administrateur invite ensuite chaque compte à s'associer en tant que compte membre dans cette région.

Un compte peut être un compte membre de plusieurs graphes de comportement dans la même région. Un compte ne peut être le compte administrateur que d'un graphe de comportement par région. Un compte peut être un compte administrateur dans différentes régions.

Alignement des comptes d'administrateur avec Security Hub et GuardDuty

Pour garantir le bon GuardDuty fonctionnement des intégrations avec Amazon AWS Security Hub et Amazon, nous recommandons que le même compte soit le compte administrateur de tous ces services.

Consultez the section called “Alignement recommandé avec GuardDuty et AWS Security Hub”.

Octroi des autorisations requises pour les comptes administrateurs

Pour vous assurer qu'un compte administrateur dispose des autorisations requises pour gérer son graphe de comportement, associez la politique `AmazonDetectiveFullAccess` gérée au IAM principal.

Faire apparaître les mises à jour de l’organisation dans Detective

Les modifications apportées à une organisation n’apparaissent pas immédiatement dans Detective.

Pour la plupart des modifications, telles que la création ou la suppression de comptes d’entreprise, la notification de Detective peut prendre jusqu’à une heure.

Une modification du compte administrateur Detective désigné dans Organizations prend moins de temps à se propager.

Utilisation des Organisations pour gérer les comptes de graphes comportementaux

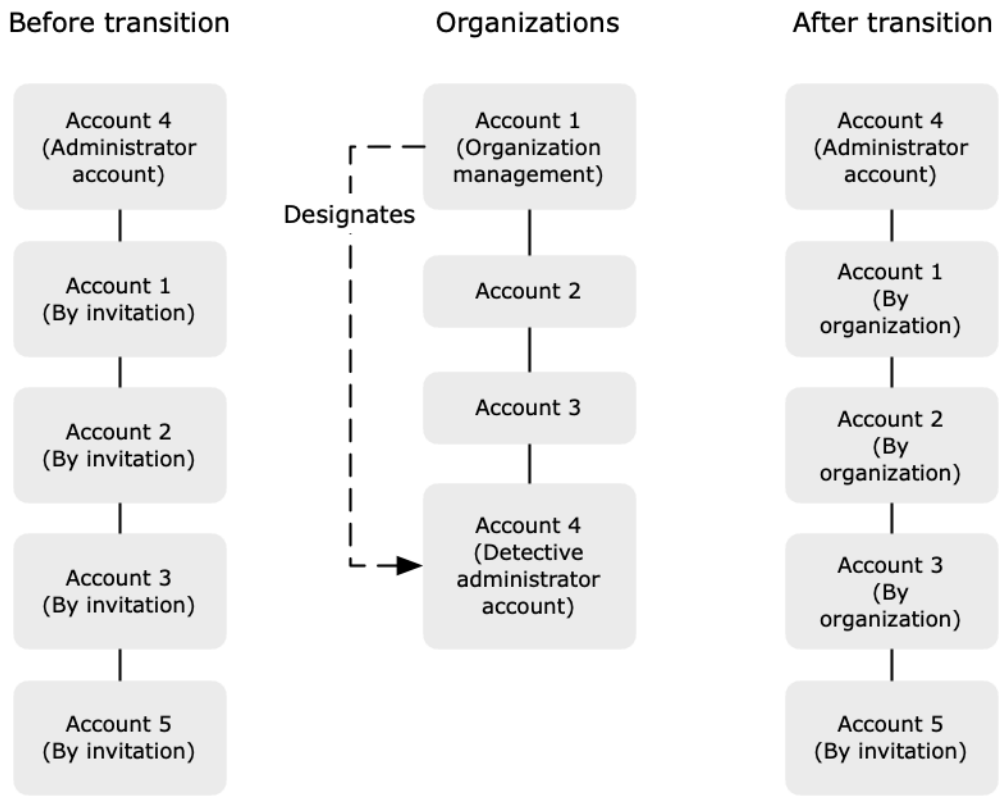
Il se peut que vous disposiez d’un graphe de comportement avec des comptes membres qui ont accepté une invitation manuelle. Si vous êtes inscrit AWS Organizations, suivez les étapes ci-dessous pour utiliser Organizations afin d'activer et de gérer les comptes des membres au lieu d'utiliser le processus d'invitation manuel :

1. Désignez le compte administrateur Detective de votre organisation. Cela crée le graphe de comportement de l’organisation.

   Si le compte administrateur Detective possède déjà un graphe de comportement, celui-ci devient le graphe de comportement de l’organisation.
2. Active les nouveaux comptes de l’organisation en tant que comptes membres dans le graphe de comportement de l’organisation.

Si le graphe de comportement de l'organisation comporte des comptes membres existants qui sont des comptes de l'organisation, ces comptes sont automatiquement activés.

Le schéma suivant montre une vue d'ensemble d'une structure de graphe de comportement avant la transition, de la configuration dans Organizations, et de la structure de compte d'un graphe de comportement après la transition.



Désignez un compte administrateur Detective pour votre organisation

Le compte de gestion de votre organisation désigne le compte administrateur Detective de votre organisation. Consultez the section called "Désignation du compte administrateur Detective".

Pour simplifier la transition, Detective vous recommande de choisir un compte administrateur actuel comme compte administrateur Detective pour l'organisation.

S'il existe un compte administrateur délégué pour Detective dans Organizations, vous devez utiliser ce compte ou le compte de gestion de l'organisation comme compte administrateur Detective.

Sinon, la première fois que vous désignez un compte administrateur Detective qui n'est pas le compte de gestion de l'organisation, Detective appelle Organizations pour faire de ce compte le compte administrateur délégué de Detective.

Activer les comptes de l'organisation en tant que comptes membres

Le compte administrateur Detective est le compte administrateur d'un graphe de comportement. Le compte administrateur Detective choisit les comptes de l'organisation à activer comme comptes membres dans le graphe de comportement de l'organisation. Consultez the section called "Gestion des comptes membres de l'organisation".

Sur la page Comptes, le compte administrateur Detective affiche tous les comptes de l'organisation.

Si le compte administrateur Detective était déjà le compte administrateur d'un graphe de comportement, ce graphe de comportement devient le graphe de comportement de l'organisation. Les comptes de l'organisation qui étaient déjà des comptes membres dans ce graphe de comportement sont activés automatiquement en tant que comptes membres. Les comptes des autres organisations ont le statut Non membre.

Les comptes de l'organisation sont de type Par organisation, même s'il s'agissait auparavant de comptes membres sur invitation.

Les comptes membres qui n'appartiennent pas à l'organisation sont de type Par invitation.

La page Gestion des comptes propose également une option, Activer automatiquement les nouveaux comptes de l'organisation, pour activer automatiquement les nouveaux comptes lorsqu'ils sont ajoutés à une organisation. Consultez the section called "Activation de nouveaux comptes d'organisation". L'option est initialement désactivée.

Lorsque le compte administrateur Detective affiche pour la première fois la page de gestion des comptes, il affiche un message contenant le bouton Activer tous les comptes de l'organisation. Lorsque vous sélectionnez Activer tous les comptes de l'organisation, Detective effectue les actions suivantes :

- Active tous les comptes actuels de l'organisation en tant que comptes membres.
- Active l'option permettant d'activer automatiquement les nouveaux comptes de l'organisation.

Il existe également l'option Activer tous les comptes de l'organisation dans la liste des comptes membres.

Désignation de l'administrateur Detective d'une organisation

Dans le graphe de comportement de l’organisation, le compte administrateur Detective gère l’appartenance au graphe de comportement pour tous les comptes de l’organisation.

Comment est géré le compte administrateur Detective : le compte de gestion de l'organisation désigne le compte administrateur Detective pour l'organisation de chaque organisation Région AWS.

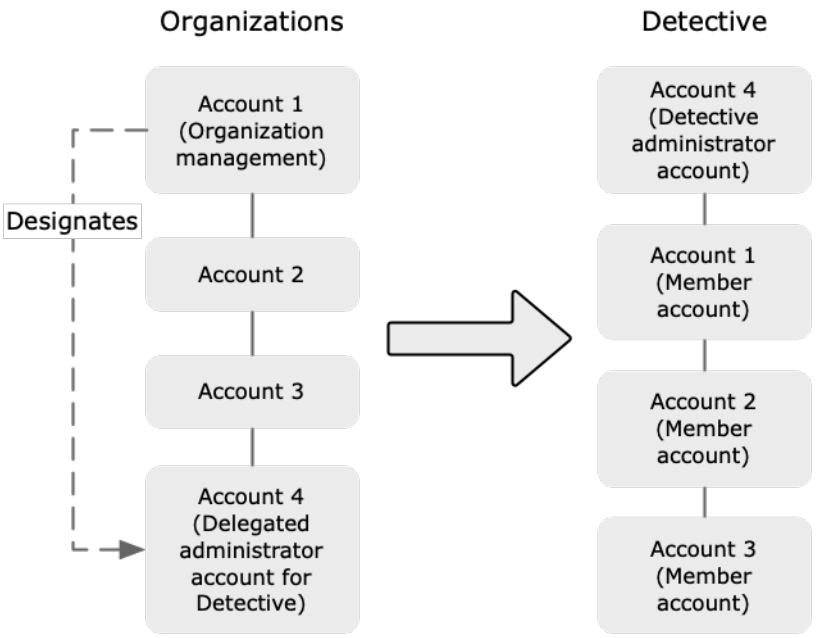
Configuration du compte administrateur Detective comme compte administrateur délégué — Le compte administrateur Detective devient également le compte administrateur délégué de Detective dans AWS Organizations. L'exception est si le compte de gestion de l'organisation se désigne comme le compte administrateur Detective. Le compte de gestion de l’organisation ne peut pas être un administrateur délégué dans Organizations.

Une fois le compte administrateur délégué défini dans Organizations, le compte de gestion de l’organisation ne peut choisir que le compte administrateur délégué ou son propre compte comme compte administrateur Detective. Nous vous recommandons de choisir le compte administrateur délégué dans toutes les régions.

Création et gestion du graphe de comportement de l'organisation : lorsque le compte de gestion de l'organisation choisit un compte administrateur Detective, Detective crée un nouveau graphe de comportement pour ce compte. Ce graphe de comportement est celui de l’organisation.

Si le compte administrateur Detective est un compte administrateur pour un graphe de comportement existant, ce graphe de comportement devient alors le graphe de comportement de l’organisation.

Le compte administrateur Detective choisit les comptes d’organisation à activer comme comptes membres dans le graphe de comportement de l’organisation.



Le compte administrateur Detective peut également envoyer des invitations à des comptes n'appartenant pas à l'organisation. Pour plus d'informations, consultez the section called "Gestion des comptes membres de l'organisation" et the section called "Gestion des comptes membres".

Autorisations requises pour configurer le compte administrateur Detective : pour vous assurer que le compte de gestion de l'organisation est en mesure de configurer le compte administrateur Detective, vous pouvez associer la politique `AmazonDetectiveOrganizationsAccess` gérée à votre AWS Identity and Access Management (IAM) entités.

Désignation d'un administrateur Detective

Le compte de gestion de l'organisation peut utiliser la console Detective pour désigner le compte administrateur Detective.

Il n'est pas nécessaire d'activer Detective pour gérer le compte administrateur Detective. Vous pouvez gérer le compte administrateur Detective depuis la page Activation Detective.

Enable Detective page (Console)

Pour désigner un administrateur Detective depuis la page Enable Detective, procédez comme suit.

1. Ouvrez la console Amazon à l'adresse https://console.aws.amazon.com/detective/.
2. Choisissez Get started (Démarrer).

3. Dans le volet Autorisations requises pour les comptes administrateurs, accordez les autorisations nécessaires au compte de votre choix afin qu'il puisse fonctionner en tant qu'administrateur Detective avec un accès complet à toutes les actions de Detective. Pour opérer en tant qu'administrateur, nous vous recommandons d'associer la politique `AmazonDetectiveFullAccess` au principal.
4. Choisissez Attach policy from IAM pour afficher la politique recommandée directement dans la IAM console.
5. Selon que vous disposez ou non d'autorisations dans la IAM console, procédez comme suit :

   - Si vous êtes autorisé à opérer dans la IAM console, associez la politique recommandée au principal que vous utilisez pour Detective.
   - Si vous n'êtes pas autorisé à opérer dans la IAM console, copiez le nom de ressource Amazon (ARN) de la politique et communiquez-le à votre IAM administrateur. Il peut ensuite associer la police en votre nom.
6. Sous Administrateur délégué, choisissez le compte administrateur Detective.

   Les options disponibles varient selon que vous disposez ou non d'un compte administrateur délégué pour Detective dans Organizations.

   - Si vous ne possédez pas de compte administrateur délégué pour Detective dans Organizations, entrez l'identifiant du compte pour le désigner comme compte administrateur Detective.

     Il se peut que vous disposiez déjà d'un compte administrateur et d'un graphe de comportement issus du processus d'invitation manuel. Dans ce cas, nous vous recommandons de désigner ce compte comme compte administrateur Detective.

     Si vous disposez d'un compte d'administrateur délégué dans Organizations for Amazon GuardDuty, AWS Security Hub, ou Amazon Macie, puis Detective vous invite à sélectionner l'un de ces comptes. Vous pouvez également saisir un autre compte.
   - Si vous disposez d'un compte administrateur délégué pour Detective dans Organizations, vous êtes invité à choisir ce compte ou le vôtre. Nous vous recommandons de choisir le compte administrateur délégué dans toutes les régions.
7. Choisisssez Delegate (Déléguer).

Si Detective est activé ou si vous êtes membre d'un graphe de comportement existant, vous pouvez désigner le compte administrateur Detective sur la page Général.

General page (Console)

Pour désigner un administrateur Detective depuis la page Général, procédez comme suit.

1. Ouvrez la console Amazon à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, sous Paramètres, choisissez Général.
3. Dans le volet des politiques gérées, vous pouvez en savoir plus sur toutes les politiques gérées prises en charge par Detective. Vous pouvez accorder les autorisations nécessaires à un compte en fonction des actions que vous souhaitez que les utilisateurs effectuent dans Detective. Pour opérer en tant qu'administrateur, nous vous recommandons d'associer la politique `AmazonDetectiveFullAccess` au principal.
4. Selon que vous disposez ou non d'autorisations dans la IAM console, procédez comme suit :

   - Si vous êtes autorisé à opérer dans la IAM console, associez la politique recommandée au principal que vous utilisez pour Detective.
   - Si vous n'êtes pas autorisé à opérer dans la IAM console, copiez le nom de ressource Amazon (ARN) de la politique et communiquez-le à votre IAM administrateur. Il peut ensuite associer la police en votre nom.

   Les options disponibles varient selon que vous disposez ou non d'un compte administrateur délégué pour Detective dans Organizations.

   - Si vous ne possédez pas de compte administrateur délégué pour Detective dans Organizations, entrez l'identifiant du compte pour le désigner comme compte administrateur Detective.

     Il se peut que vous disposiez déjà d'un compte administrateur et d'un graphe de comportement issus du processus d'invitation manuel. Dans ce cas, nous vous recommandons de désigner ce compte comme compte administrateur Detective.

     Si vous disposez d'un compte d'administrateur délégué dans Organizations for Amazon GuardDuty, AWS Security Hub, ou Amazon Macie, puis Detective vous invite à sélectionner l'un de ces comptes. Vous pouvez également saisir un autre compte.
   - Si vous disposez d'un compte administrateur délégué pour Detective dans Organizations, vous êtes invité à choisir ce compte ou le vôtre. Nous vous recommandons de choisir le compte administrateur délégué dans toutes les régions.
5. Choisisssez Delegate (Déléguer).

Detective API, AWS CLI

Pour désigner le compte administrateur du Detective, vous pouvez utiliser un API appel ou AWS Command Line Interface. Vous devez utiliser les informations d'identification du compte de gestion de l'organisation.

Si vous possédez déjà un compte administrateur délégué pour Detective dans les organisations, vous devez choisir ce compte ou le vôtre. Nous vous recommandons de choisir le compte administrateur délégué.

Pour désigner le compte administrateur Detective (DetectiveAPI, AWS CLI)

- Detective API : Utilisez l'`EnableOrganizationAdminAccount`opération. Vous devez fournir le AWS identifiant du compte administrateur du Detective. Pour obtenir l'identifiant du compte, utilisez l'opération `ListOrganizationAdminAccounts`.
- AWS CLI: Sur la ligne de commande, exécutez la `enable-organization-admin-account`commande.

```
aws detective enable-organization-admin-account --account-id <admin account ID>
```

Exemple

```
aws detective enable-organization-admin-account --account-id 777788889999
```

Suppression du compte administrateur Detective

Le compte de gestion de l'organisation peut supprimer le compte administrateur Detective actuel dans une région. Lorsque vous supprimez le compte administrateur Detective, Detective le supprime uniquement de la région actuelle. Cela ne modifie pas le compte administrateur délégué dans Organizations.

Lorsque le compte de gestion de l'organisation supprime le compte administrateur Detective dans une région, Detective supprime le graphe de comportement de l'organisation. Detective est désactivé pour le compte administrateur Detective supprimé.

Pour supprimer le compte administrateur délégué actuel pour Detective, vous devez utiliser les OrganizationsAPI. Lorsque vous supprimez le compte administrateur délégué pour Detective dans Organizations, Detective supprime tous les graphes de comportement de l'organisation dans

lesquels le compte administrateur délégué est le compte administrateur Detective. Les graphes de comportement de l'organisation dont le compte de gestion de l'organisation est le compte administrateur Detective ne sont pas affectés.

Console

Depuis la console Detective, vous pouvez supprimer le compte administrateur Detective.

Lorsque vous supprimez le compte administrateur Detective, Detective est désactivé pour le compte et le graphe du comportement de l'organisation est supprimé. Le compte administrateur Detective est supprimé uniquement dans la région actuelle.

> **Important**
>
> La suppression d'un compte administrateur Detective n'affecte pas le compte administrateur délégué dans Organizations.

Pour supprimer le compte administrateur Detective (page Activation Detective)

1. Ouvrez la console Amazon Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Choisissez Get started (Démarrer).
3. Sous Administrateur délégué, choisissez Désactiver Amazon Detective.
4. Dans la boîte de dialogue de confirmation, saisissez **`disable`**, puis choisissez Désactiver Amazon Detective.

Pour supprimer un compte administrateur Detective (page Général)

1. Ouvrez la console Amazon Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, sous Paramètres, choisissez Général.
3. Sous Administrateur délégué, choisissez Désactiver Amazon Detective.
4. Dans la boîte de dialogue de confirmation, saisissez **`disable`**, puis choisissez Désactiver Amazon Detective.

Detective API, AWS CLI

Pour supprimer le compte administrateur Detective, vous pouvez utiliser un API appel ou AWS CLI. Vous devez utiliser les informations d'identification du compte de gestion de l'organisation.

Lorsque vous supprimez le compte administrateur Detective, Detective est désactivé pour le compte et le graphe du comportement de l'organisation est supprimé.

> **Important**
>
> La suppression d'un compte administrateur Detective n'affecte pas le compte administrateur délégué dans Organizations.

Pour supprimer le compte administrateur Detective (DetectiveAPI, AWS CLI)

- Detective API : Utilisez l'`DisableOrganizationAdminAccount`opération.

  Lorsque vous utilisez le Detective API pour supprimer le compte administrateur du Detective, celui-ci n'est supprimé que dans la région où l'APIappel ou la commande a été émis.
- AWS CLI: Sur la ligne de commande, exécutez la `disable-organization-admin-account`commande.

```
aws detective disable-organization-admin-account
```

Supprimer le compte d'administrateur délégué

La suppression du compte administrateur Detective ne supprime pas automatiquement le compte administrateur délégué dans Organizations. Pour supprimer le compte d'administrateur délégué pour Detective, vous pouvez utiliser les OrganizationsAPI.

Lorsque vous supprimez le compte administrateur délégué, cela supprime tous les graphes de comportement de l'organisation dans lesquels le compte administrateur délégué est le compte administrateur Detective. Cela désactive également Detective pour le compte dans ces régions.

Pour supprimer le compte d'administrateur délégué (OrganizationsAPI, AWS CLI)

- Organisations API : utilisez l'`DeregisterDelegatedAdministrator`opération. Vous devez fournir l'identifiant du compte administrateur Detective et le principal du service Detective, qui est `detective.amazonaws.com`.
- AWS CLI: Sur la ligne de commande, exécutez la `deregister-delegated-administrator`commande.

```
aws organizations deregister-delegated-administrator --account-id <Detective
 administrator account ID> --service-principal <Detective service principal>
```

Exemple

```
aws organizations deregister-delegated-administrator --account-id 777788889999 --
service-principal detective.amazonaws.com
```

Actions disponibles pour les comptes

Les comptes administrateurs et les comptes membres ont accès aux actions Detective suivantes. Dans le tableau, les valeurs ont les significations suivantes :

- N'importe lequel : le compte peut effectuer l'action pour tous les comptes du même compte administrateur Detective.
- Auto-utilisateur : le compte ne peut effectuer l'action que pour son propre compte.
- Tiret (–) : le compte ne peut pas effectuer l'action.

Dans le graphe de comportement de l'organisation, le compte administrateur Detective détermine les comptes de l'organisation à activer comme comptes membres. Ils peuvent configurer Detective pour qu'il active automatiquement les nouveaux comptes de l'organisation comme comptes membres, ou ils peuvent activer les comptes de l'organisation manuellement.

Un compte administrateur peut inviter des comptes à devenir des comptes membres dans le graphe de comportement. Lorsqu'un compte membre accepte l'invitation et qu'il est activé, Amazon Detective commence l'ingestion et l'extraction des données du compte membre dans ce graphe de comportement.

Pour les graphes de comportement autres que le graphe de comportement de l'organisation, tous les comptes membres sont des comptes invités.

Le tableau suivant indique les autorisations par défaut pour les comptes administrateurs et les comptes membres. Vous pouvez utiliser des IAM politiques personnalisées pour restreindre davantage l'accès aux fonctionnalités et fonctions de Detective.

Action	Compte administrateur (organisation)	Compte administrateur (invitation)	Membre (organisation)	Membre (invitation)
Afficher les comptes	N'importe quel compte	N'importe quel compte	Auto-utilisateur (Afficher les comptes administrateurs)	Auto-utilisateur (Afficher les comptes administrateurs)
Supprimer un compte membre	N'importe quel compte Les comptes invités sont supprimés Les comptes de l'organisation sont dissociés	N'importe quel compte	–	Auto-utilisateur
Ajouter ou supprimer des packages de sources de données facultatifs	N'importe quel compte (le paramètre s'applique à tous les comptes membres)	N'importe quel compte (le paramètre s'applique à tous les comptes membres)	–	–
Désactivation de Detective	Auto-utilisateur	Auto-utilisateur	–	–
Afficher les données du graphe de comportement	N'importe quel compte	N'importe quel compte	–	–
Activer ou désactiver les packages de	Tous	Tous	–	–

Action	Compte administrateur (organisation)	Compte administrateur (invitation)	Membre (organisation)	Membre (invitation)
sources de données facultatifs				

Consulter la liste des comptes

Le compte administrateur peut utiliser la console Detective ou API consulter la liste des comptes. Cellec-ci peut inclure :

- Les comptes ayant été invités par le compte administrateur à rejoindre le graphe de comportement. Ces comptes sont de type Par invitation.
- Pour le graphe de comportement d'organisation, tous les comptes de l'organisation. Ces comptes sont de type Par organisation.

Les résultats n'incluent pas les comptes membres invités qui ont refusé une invitation, ou que le compte administrateur a supprimé du graphe de comportement. Ils incluent uniquement les comptes avec les statuts suivants.

Vérification en cours

Pour les comptes invités, Detective vérifie l'adresse e-mail du compte avant d'envoyer l'invitation.

Pour les comptes de l'organisation, Detective vérifie que le compte appartient à l'organisation. Detective vérifie également que c'est le compte administrateur du Detective qui a activé le compte.

La vérification a échoué

La vérification a échoué. L'invitation n'a pas été envoyée, ou le compte de l'organisation n'a pas été activé en tant que membre.

Invité

Pour les comptes invités. L'invitation a été envoyée, mais le compte membre n'a pas encore répondu.

Pas un membre

Pour les comptes de l'organisation figurant dans le graphe de comportement de l'organisation. Le compte de l'organisation n'est pas actuellement un compte membre. Il ne fournit pas de données au graphe du comportement de l'organisation.

Activées

Pour les comptes invités, le compte membre a accepté l'invitation et fournit des données au graphe de comportement.

Pour les comptes de l'organisation figurant dans le graphe du comportement de l'organisation, le compte administrateur Detective a activé le compte en tant que compte membre. Le compte fournit des données au graphe du comportement de l'organisation.

Non activé

Pour les comptes invités, le compte membre a accepté l'invitation, mais ne peut pas être activé.

Pour les comptes de l'organisation figurant dans le graphe de comportement de l'organisation, le compte administrateur Detective a essayé d'activer le compte, mais celui-ci n'a pas pu être activé.

Pour les comptes invités, Detective vérifie le nombre de comptes membres. Le nombre maximum de comptes membres pour un graphe de comportement est de 1 200. Si le graphe de comportement contient déjà 1 200 comptes membres, les nouveaux comptes ne peuvent pas être activés.

Detective vérifie si votre volume de données se situe dans les limites du quota de Detective. Le volume de données entrant dans un graphe de comportement doit être inférieur au maximum autorisé par Detective. Si le volume actuellement ingéré est supérieur à la limite de 10 To par jour pour le volume de données du Behavior Graph, Detective ne vous autorisera pas à ajouter de comptes membres supplémentaires.

Listing des comptes (console)

Vous pouvez utiliser le AWS Management Console pour consulter et filtrer votre liste de comptes.

Pour afficher la liste des comptes (console)

1. Connectez-vous au AWS Management Console. Ouvrez ensuite la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, choisissez Gestion des comptes.

La liste des comptes membres contient les comptes suivants :

- Votre compte
- Comptes auxquels vous avez demandé de fournir des données au graphe de comportement
- Dans le graphe du comportement de l'organisation, tous les comptes de l'organisation

Pour chaque compte, la liste affiche les informations suivantes :

- L'identifiant AWS du compte.
- Pour les comptes de l'organisation, le nom du compte.
- Type de compte (par invitation ou par organisation).
- Adresse e-mail de l'utilisateur racine du compte.
- État du compte.
- Volume quotidien de données du compte. Detective ne peut pas récupérer le volume de données pour les comptes qui ne sont pas activés en tant que comptes membres.
- Date de la dernière mise à jour du flux.

Vous pouvez utiliser les onglets situés en haut du tableau pour filtrer la liste en fonction du statut du compte membre. Chaque onglet indique le nombre de comptes membres correspondants.

- Choisissez Tout pour afficher tous les comptes membres.
- Choisissez Activé pour afficher les comptes dont le statut est Activé.
- Choisissez Non activé pour afficher les comptes dont le statut est Non activé.

Vous pouvez également ajouter d'autres filtres à la liste des comptes des membres.

Pour ajouter un filtre à la liste des comptes dans le graphe de comportement (console)

1. Choisissez la zone de filtre.
2. Choisissez la colonne que vous souhaitez utiliser pour filtrer la liste.
3. Pour la colonne spécifiée, choisissez la valeur à utiliser pour le filtre.
4. Pour supprimer un filtre, choisissez l'icône x en haut à droite.
5. Pour mettre la liste à jour avec les informations d'état les plus récentes, choisissez l'icône d'actualisation en haut à droite.

Répertorier vos comptes de membres (DetectiveAPI, AWS CLI)

Vous pouvez utiliser un API appel ou le AWS Command Line Interface pour afficher la liste des comptes des membres dans votre graphique de comportement.

Pour obtenir le graphe ARN de votre comportement à utiliser dans la requête, utilisez l'`ListGraphs`opération.

Pour récupérer la liste des comptes des membres (DetectiveAPI, AWS CLI)

- Detective API : Utilisez l'`ListMembers`opération. Pour identifier le graphe de comportement souhaité, spécifiez le graphe de comportementARN.

  Notez que le graphe de comportement de l'organisation `ListMembers` ne renvoie pas les comptes de l'organisation que vous n'avez pas activés en tant que comptes membres ou que vous avez dissociés du graphe de comportement.
- AWS CLI: À l'invite de commande, exécutez la commande `list-members`.

  ```
  aws detective list-members --graph-arn <behavior graph ARN>
  ```

  Exemple :

  ```
  aws detective list-members --graph-arn arn:aws:detective:us-
  east-1:111122223333:graph:123412341234
  ```

Pour récupérer des informations sur des comptes de membres spécifiques dans votre graphique de comportement (DetectiveAPI, AWS CLI)

- Detective API : Utilisez l'`GetMembers`opération. Spécifiez le graphe de comportement ARN et la liste des identifiants de compte pour les comptes des membres.
- AWS CLI: À l'invite de commande, exécutez la commande `get-members`.

  ```
  aws detective get-members --account-ids <member account IDs> --graph-arn <behavior
   graph ARN>
  ```

  Exemple :

```
aws detective get-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Gérer les comptes de l'organisation en tant que comptes membres de Detective

Dans le graphe de comportement de l'organisation, le compte administrateur Detective détermine les comptes de l'organisation à activer comme comptes membres. Par défaut, les nouveaux comptes de l'organisation ne sont pas activés en tant que comptes membres. Leur statut est Non membre. Le compte administrateur Detective peut configurer Detective pour qu'il active automatiquement de nouveau comptes de l'organisation en tant que comptes membres dans le graphe de comportement d'organisation.

L'administrateur de Detective peut configurer Detective pour activer automatiquement les nouveaux comptes d'organisation en tant que comptes membres. Lorsque vous choisissez d'activer automatiquement les comptes de l'organisation, Detective commence à activer les nouveaux comptes comme comptes membres à mesure qu'ils sont ajoutés à l'organisation. Detective n'active pas les comptes de l'organisation existants qui ne sont pas encore activés.

The Detective peut activer manuellement les comptes d'organisation en tant que comptes de membres, si vous ne souhaitez pas activer automatiquement les nouveaux comptes d'organisation. Ils peuvent également activer manuellement des comptes d'organisation dissociés. L'administrateur du Detective ne peut pas activer un compte d'organisation en tant que compte membre si le graphe de comportement de l'organisation contient déjà un maximum de 1 200 comptes activés. Dans ce cas, le statut du compte de l'organisation reste Non membre.

L'administrateur Detective peut également dissocier les comptes de l'organisation du graphe de comportement de l'organisation. Pour arrêter l'ingestion des données d'un compte de l'organisation dans le graphe de comportement de l'organisation, vous pouvez dissocier le compte. Les données existantes pour ce compte restent dans le graphe de comportement.

Table des matières

- Activation de nouveaux comptes d'organisation en tant que comptes membres de Detective
- Activation des comptes d'organisation en tant que comptes membres de Detective
- Dissocier les comptes d'organisation en comptes membres de Detective

Activation de nouveaux comptes d'organisation en tant que comptes membres de Detective

Le compte administrateur Detective peut configurer Detective pour qu'il active automatiquement de nouveau comptes de l'organisation en tant que comptes membres dans le graphe de comportement d'organisation.

Lorsque de nouveaux comptes sont ajoutés à votre organisation, ils sont ajoutés à la liste de la page de Gestion des comptes. Pour les comptes de l'organisation, le type est Par organisation.

Par défaut, les nouveaux comptes de l'organisation ne sont pas activés en tant que comptes membres. Leur statut est Non membre.

Lorsque vous choisissez d'activer automatiquement les comptes de l'organisation, Detective commence à activer les nouveaux comptes comme comptes membres à mesure qu'ils sont ajoutés à l'organisation. Detective n'active pas les comptes de l'organisation existants qui ne sont pas encore activés.

Detective peut activer les comptes d'organisation en tant que comptes membres uniquement si le nombre maximum de comptes de membres pour un graphique de comportement est de 1 200. Si votre graphe de comportement contient déjà 1 200 comptes membres, les nouveaux comptes ne peuvent pas être activés.

Console

Sur la page Gestion des comptes, le paramètre Activer automatiquement les nouveaux comptes de l'organisation détermine s'il faut activer automatiquement les comptes lorsqu'ils sont ajoutés à une organisation.

Pour activer automatiquement de nouveaux comptes de l'organisation comme comptes membres

1. Ouvrez la console Amazon Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, choisissez Gestion de comptes.
3. Régler l'option Activer automatiquement les nouveaux comptes de l'organisation en position activée.

DetectiveAPI/AWS CLI

Pour déterminer s'il convient d'activer automatiquement les nouveaux comptes d'organisation en tant que comptes membres de Detective, le compte administrateur peut utiliser le Detective API ou le AWS Command Line Interface.

Pour afficher et gérer la configuration, vous devez fournir le graphe de comportementARN. Pour l'obtenirARN, utilisez l'`ListGraphs`opération.

Pour afficher la configuration actuelle d'activation automatique des comptes de l'organisation

- Detective API : Utilisez l'`DescribeOrganizationConfiguration`opération.

  Dans la réponse, si les nouveaux comptes de l'organisation sont activés automatiquement, alors `AutoEnable` est `true`.
- AWS CLI: À l'invite de commande, exécutez la commande `describe-organization-configuration`.

```
aws detective describe-organization-configuration --graph-arn <behavior graph ARN>
```

  Exemple

```
aws detective describe-organization-configuration --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Pour activer automatiquement de nouveaux comptes de l'organisation

- Detective API : Utilisez l'`UpdateOrganizationConfiguration`opération. Pour activer automatiquement de nouveaux comptes de l'organisation, définissez `AutoEnable` sur `true`.
- AWS CLI: À l'invite de commande, exécutez la commande `update-organization-configuration`.

```
aws detective update-organization-configuration --graph-arn <behavior graph ARN>
 --auto-enable | --no-auto-enable
```

  Exemple

```
aws detective update-organization-configuration --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --auto-enable
```

Activation des comptes d'organisation en tant que comptes membres de Detective

Si vous n'activez pas automatiquement les nouveaux comptes de l'organisation, vous pouvez les activer manuellement. Vous devez également activer manuellement les comptes que vous avez dissociés.

Détermination de la capacité d'un compte à être activé

Vous ne pouvez pas activer un compte de l'organisation en tant que compte membre si le graphe de comportement de l'organisation comporte déjà le nombre maximum de 1 200 comptes activés. Dans ce cas, le statut du compte de l'organisation reste Non membre. Le compte ne fournit aucune donnée au graphe de comportement.

Dès que le compte membre peut être activé, Detective fait passer automatiquement le statut du compte membre à Activé. Par exemple, le statut du compte membre passe à Activé si le compte administrateur supprime d'autres comptes membres pour libérer de la place pour un compte.

Console

Sur la page Gestion des comptes, vous pouvez activer les comptes de l'organisation en tant que comptes membres.

Pour activer les comptes de l'organisation en tant que comptes membres

1. Ouvrez la console Amazon Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, choisissez Gestion de comptes.
3. Pour afficher la liste des comptes qui ne sont pas activés actuellement, choisissez Non activé.
4. Vous pouvez sélectionner des comptes de l'organisation spécifiques ou activer tous les comptes de l'organisation.

   Pour activer les comptes de l'organisation sélectionnés :

a. Sélectionnez chaque compte de l'organisation que vous souhaitez activer.

b. Choisissez Activer les comptes.

Pour activer tous les comptes de l'organisation, choisissez Activer tous les comptes de l'organisation.

Detective API/AWS CLI

Vous pouvez utiliser le Detective API ou le AWS Command Line Interface pour activer les comptes d'organisation en tant que comptes de membres dans le graphique du comportement de l'organisation. Pour obtenir le graphe ARN de votre comportement à utiliser dans la requête, utilisez l'`ListGraphs`opération.

Pour activer les comptes de l'organisation en tant que comptes membres

- Detective API : Utilisez l'`CreateMembers`opération. Vous devez fournir le graphiqueARN.

  Pour chaque compte, spécifiez l'identifiant du compte. Les comptes de l'organisation figurant dans le graphe de comportement de l'organisation ne reçoivent aucune invitation. Il n'est pas nécessaire de fournir une adresse e-mail ou d'autres informations d'invitation.
- AWS CLI: À l'invite de commande, exécutez la commande `create-members`.

```
aws detective create-members --accounts AccountId=<AWS account ID> --graph-
arn <behavior graph ARN>
```

Exemple

```
aws detective create-members --accounts AccountId=444455556666
 AccountId=123456789012 --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Dissocier les comptes d'organisation en comptes membres de Detective

Pour arrêter l'ingestion des données d'un compte de l'organisation dans le graphe de comportement de l'organisation, vous pouvez dissocier le compte. Les données existantes pour ce compte restent dans le graphe de comportement.

Lorsque vous dissociez le compte d'une organisation, le statut passe à Non membre. Detective arrête l'ingestion des données de ce compte, mais le compte reste dans la liste.

Console

À partir de la page Gestion des comptes, vous pouvez dissocier les comptes de l'organisation en tant que comptes membres.

1. Ouvrez la console Amazon Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, choisissez Gestion de comptes.
3. Pour afficher la liste des comptes activés, choisissez Activé.
4. Activez la case à cocher pour chaque compte à dissocier.
5. Choisissez Actions. Choisissez ensuite Désactiver les comptes.

   Le statut des comptes dissociés passe à Non membre.

Detective API/AWS CLI

Pour obtenir le graphe ARN de votre comportement à utiliser dans la requête, utilisez l'`ListGraphs`opération.

Pour dissocier les comptes d'organisation du graphe de comportement de l'organisation

- Detective API : Utilisez l'`DeleteMembers`opération. Spécifiez le graphique ARN et la liste des identifiants de compte pour les comptes des membres à dissocier.
- AWS CLI: À l'invite de commande, exécutez la commande `delete-members`.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

Exemple

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Gérer les comptes des membres invités dans Detective

Un compte administrateur Detective peut inviter des comptes à devenir des comptes membres dans son graphe de comportement. Un graphe de comportement peut contenir jusqu'à 1 200 comptes membres. Lorsqu'un compte membre accepte l'invitation et qu'il est activé, Amazon Detective commence l'ingestion et l'extraction des données du compte membre dans ce graphe de comportement.

Pour inviter des comptes individuels, vous pouvez spécifier manuellement les comptes des membres à inviter à ajouter leurs données à un graphique de comportement. Si vous souhaitez ajouter une liste de comptes membres, vous pouvez choisir de fournir un fichier .csv contenant une liste de comptes membres à inviter sur votre graphique de comportement.

Pour les graphes de comportement autres que le graphique de comportement de l'organisation, tous les comptes membres sont des comptes invités. Le compte administrateur Detective peut également inviter des comptes qui ne sont pas des comptes d'organisation sur le graphe de comportement de l'organisation.

À un niveau élevé, le processus pour inviter des comptes à contribuer à un graphe de comportement est le suivant.

1. Pour chaque compte membre à ajouter, le compte administrateur fournit l'identifiant du AWS compte et l'adresse e-mail de l'utilisateur root.
2. Detective vérifie que l'adresse e-mail est bien celle de l'utilisateur racine du compte. Si les informations du compte sont valides, Detective envoie l'invitation au compte membre.

   Detective n'effectue pas cette validation et n'envoie pas d'invitations par e-mail aux comptes des membres dans les régions suivantes :

   - AWS GovCloud Région (USA Est)
   - AWS GovCloud Région (US-Ouest)

   Pour les autres régions, vous pouvez `DisableEmailNotification` utiliser le CreateMembersfonctionnement du DetectiveAPI. S'il `DisableEmailNotification` est défini sur true, Detective n'enverra pas d'invitations aux comptes des membres. Ce paramètre est utile pour les comptes gérés de manière centralisée.
3. Le compte membre accepte ou refuse l'invitation.

Même si le compte administrateur n'envoie pas d'e-mails d'invitation, le compte membre doit tout de même répondre à l'invitation.

4. Une fois que le compte membre a accepté l'invitation, Detective commence à intégrer les données du compte membre dans le graphe de comportement.
5. Dès que le compte membre peut être activé, Detective fait passer automatiquement le statut du compte membre à Activé.

   Par exemple, le statut du compte membre passe à Activé si le compte administrateur supprime d'autres comptes membres pour libérer de la place pour un compte.

   Si plusieurs comptes sont Non activés, Detective active ces comptes dans l'ordre dans lequel ils ont été invités. Le processus permettant de vérifier s'il faut activer des comptes Non activés s'exécute toutes les heures.

   Le compte administrateur peut également activer les comptes manuellement, au lieu d'attendre le processus automatique. Par exemple, le compte administrateur peut souhaiter sélectionner les comptes à activer. Pour plus d'informations sur la façon d'activer un compte de membre, consultezthe section called "Activation d'un compte membre non activé".

   Veuillez noter que Detective a commencé à activer automatiquement les comptes Non activés le 12 mai 2021. Les comptes Non activés alors ne sont pas activés automatiquement. Le compte administrateur doit les activer manuellement.

Le compte administrateur peut supprimer des comptes membres invités du graphe de comportement. Detective ne supprime aucune donnée existante du graphe de comportement, qui regroupe les données des comptes membres.

Table des matières

- Inviter des comptes individuels à accéder à un graphique de comportement
- Inviter une liste de comptes membres à un graphique de comportement
- Activation d'un compte membre non activé
- Supprimer les comptes de membres d'un graphique de comportement

Inviter des comptes individuels à accéder à un graphique de comportement

Vous pouvez spécifier manuellement les comptes membres à inviter, afin qu'ils apportent leur contribution à un graphe de comportement avec leurs données.

Console

Pour sélectionner manuellement les comptes membres à inviter à l'aide de la console Detective.

1. Ouvrez la console Amazon à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, choisissez Gestion de compte.
3. Choisissez Actions. Choisissez ensuite Inviter des comptes.
4. Sous Ajouter des comptes, choisissez Ajouter des comptes individuels.
5. Pour ajouter un compte membre à la liste d'invitation, effectuez les étapes suivantes.
   a. Choisissez Ajouter un compte.
   b. Pour ID de AWS compte, entrez l'ID du AWS compte.
   c. Sous Adresse e-mail, entrez l'adresse e-mail de l'utilisateur racine pour le compte.
6. Pour supprimer un compte de la liste, choisissez Supprimer ce compte.
7. Sous Personnaliser l'e-mail d'invitation, ajoutez du contenu personnalisé à inclure dans l'e-mail d'invitation.

   Par exemple, vous pouvez utiliser cette zone pour fournir des informations de contact. Vous pouvez également l'utiliser pour rappeler au compte membre qu'il doit associer la IAM politique requise à son utilisateur ou à son rôle avant de pouvoir accepter l'invitation.
8. La IAMpolitique relative aux comptes des membres contient le texte de la IAM politique requise pour les comptes des membres. L'invitation par e-mail inclut ce texte de politique. Pour copier le texte de politique, choisissez Copier.
9. Choisissez Inviter.

Detective API/AWS CLI

Vous pouvez utiliser le Detective API ou le AWS Command Line Interface pour inviter les comptes des membres à ajouter leurs données à un graphique de comportement. Pour obtenir le graphe ARN de votre comportement à utiliser dans la requête, utilisez l'`ListGraphs`opération.

Pour inviter les comptes des membres à accéder à un graphe de comportement (DetectiveAPI, AWS CLI)

- Detective API : Utilisez l'`CreateMembers`opération. Vous devez fournir le graphiqueARN. Pour chaque compte, spécifiez l'identifiant du compte et l'adresse e-mail de l'utilisateur racine.

  Pour ne pas envoyer d'e-mails d'invitation aux comptes membres, définissez le paramètre `DisableEmailNotification` sur true. Par défaut, `DisableEmailNotification` a la valeur false.

  Si vous envoyez des e-mails d'invitation, vous pouvez éventuellement fournir un texte personnalisé à ajouter à l'e-mail d'invitation.

- AWS CLI : À l'invite de commande, exécutez la commande `create-members`.

```
aws detective create-members --accounts AccountId=<AWS account
 ID>,EmailAddress=<root user email address> --graph-arn <behavior graph ARN> --
message "<Custom message text>"
```

  Exemple

```
aws detective create-members --accounts
 AccountId=444455556666,EmailAddress=mmajor@example.com
 AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234 --message "This
 is Paul Santos. I need to add your account to the data we use for security
 investigation in Amazon Detective. If you have any questions, contact me at
 psantos@example.com."
```

  Pour indiquer de ne pas envoyer d'e-mails d'invitation aux comptes membres, incluez `--disable-email-notification`.

```
aws detective create-members --accounts AccountId=<AWS account
 ID>,EmailAddress=<root user email address> --graph-arn <behavior graph ARN> --
disable-email-notification
```

  Exemple

```
aws detective create-members --accounts
 AccountId=444455556666,EmailAddress=mmajor@example.com
```

```
 AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234 --disable-email-
notification
```

Inviter une liste de comptes membres à un graphique de comportement

Depuis la console Detective, vous pouvez fournir un fichier `.csv` contenant la liste des comptes membres à inviter à accéder à votre graphe de comportement.

La première ligne du fichier est l'en-tête. Chaque compte est ensuite répertorié sur une ligne distincte. Chaque entrée de compte de membre contient l'identifiant du AWS compte et l'adresse e-mail de l'utilisateur root du compte.

Exemple :

```
Account ID,Email address
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Lorsque Detective traite le fichier, il ignore les comptes déjà invités, sauf si le statut du compte est Échec de la vérification. Ce statut indique que l'adresse e-mail fournie pour le compte ne correspond pas à l'adresse e-mail de l'utilisateur racine du compte. Dans ce cas, Detective supprime l'invitation d'origine et essaie à nouveau de vérifier l'adresse e-mail et d'envoyer l'invitation.

Cette option fournit également un modèle pouvant être utilisé pour créer la liste des comptes.

Pour inviter des comptes membres à partir d'une liste csv (console)

1. Ouvrez la console Amazon Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, choisissez Gestion de compte.
3. Choisissez Actions. Choisissez ensuite Inviter des comptes.
4. Sous Ajouter des comptes, choisissez Ajouter à partir du fichier .csv.
5. Pour télécharger un fichier modèle à partir duquel travailler, choisissez Télécharger le modèle .csv.
6. Pour sélectionner le fichier contenant la liste des comptes, choisissez Choisir un fichier .csv.
7. Sous Vérifier les comptes membres, vérifiez la liste des comptes membres que Detective a trouvés dans le fichier.

8. Sous Personnaliser l'e-mail d'invitation, ajoutez du contenu personnalisé à inclure dans l'e-mail d'invitation.

   Par exemple, vous pouvez fournir des informations de contact ou rappeler au compte membre la IAM politique requise.

9. La IAMpolitique relative aux comptes des membres contient le texte de la IAM politique requise pour les comptes des membres. L'invitation par e-mail inclut ce texte de politique. Pour copier le texte de politique, choisissez Copier.

10. Choisissez Inviter.

Ajouter une liste de comptes membres dans toutes les régions

Detective fournit un script Python open source GitHub qui vous permet d'effectuer les opérations suivantes :

- Ajoutez une liste spécifiée de comptes membres aux graphes de comportement d'un compte administrateur dans une liste spécifiée de régions.
- Si le compte administrateur ne possède pas de graphe de comportement dans une région, le script active également Detective et crée le graphe de comportement dans cette région.
- Envoyer des e-mails d'invitation aux comptes membres.
- Accepter automatiquement les invitations aux comptes membres.

Pour plus d'informations sur la configuration et l'utilisation GitHub des scripts, consultezthe section called "Scripts Python d'Amazon Detective".

Activation d'un compte membre non activé

Une fois qu'un compte membre a accepté une invitation, Amazon Detective vérifie le nombre de comptes membres. Le nombre maximum de comptes membres pour un graphe de comportement est de 1 200. Si votre graphe de comportement contient déjà 1 200 comptes membres, les nouveaux comptes ne peuvent pas être activés. Si Detective ne parvient pas à activer le compte membre, il lui attribue le statut Non activé.

Les comptes membres qui sont Non activés ne fournissent pas de données au graphe de comportement.

Detective active automatiquement les comptes dans la mesure où le graphe de comportement peut s'y adapter.

Vous pouvez également essayer d'activer manuellement les comptes membres qui sont Non activés. Par exemple, vous pouvez supprimer des comptes membres existants pour réduire le volume de données. Au lieu d'attendre le processus automatique pour activer les comptes, vous pouvez essayer d'activer les comptes membres Non activés.

Console

La liste des comptes membres inclut une option permettant d'activer certains comptes membres qui sont Non activés.

Pour activer un compte membre non activé

1. Ouvrez la console Amazon Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, choisissez Gestion de compte.
3. Sous Mes comptes membres, cochez la case correspondant à chaque compte membre à activer.

   Vous ne pouvez activer que les comptes membres dont le statut est Non activé.
4. Choisissez Activer les comptes.

Detective détermine si le compte membre peut être activé. Si le compte membre peut être activé, le statut passe à Activé.

Detective API/CLI

Vous pouvez utiliser un API appel ou le AWS Command Line Interface pour activer un compte membre unique qui n'est pas activé. Pour obtenir le graphe ARN de votre comportement à utiliser dans la requête, utilisez l'`ListGraphs`opération.

Pour activer un compte membre Non activé

- Detective API : Utilisez l'`StartMonitoringMember`APIopération. Vous devez fournir le graphe de comportementARN. Pour identifier le compte membre, utilisez l'identifiant du AWS compte.
- AWS CLI: Exécutez la `start-monitoring-member`commande.

```
start-monitoring-member --graph-arn <behavior graph ARN> --account-id <AWS account
 ID>
```

Par exemple :

```
start-monitoring-member --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --account-id 444455556666
```

Supprimer les comptes de membres d'un graphique de comportement

Le compte administrateur peut supprimer les comptes des membres invités d'un graphe de comportement à tout moment.

Detective supprime automatiquement les comptes des membres résiliés en AWS, sauf dans les AWS GovCloud régions (USA Est) et AWS GovCloud (USA Ouest).

Lorsqu'un compte membre invité est supprimé d'un graphe de comportement, les événements suivants se produisent.

- Le compte membre est supprimé de Mes comptes membres.
- Amazon Detective arrête l'ingestion des données du compte supprimé.

Detective ne supprime aucune donnée existante du graphe de comportement, qui regroupe les données des comptes membres.

Console

Vous pouvez utiliser le AWS Management Console pour supprimer les comptes de membres invités de votre graphique de comportement.

Pour supprimer des comptes membres (console)

1. Ouvrez la console Amazon Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, choisissez Gestion de compte.
3. Dans la liste des comptes, cochez la case de chaque membre à supprimer.

   Vous ne pouvez pas supprimer votre propre compte de la liste.

4. Choisissez Actions. Choisissez ensuite Désactiver les comptes.

Detective API/CLI

Vous pouvez utiliser le Detective API ou le AWS Command Line Interface pour supprimer les comptes de membres invités de votre graphe de comportement. Pour obtenir le graphe ARN de votre comportement à utiliser dans la requête, utilisez l'`ListGraphs`opération.

Pour supprimer les comptes de membres invités de votre graphe de comportement (DetectiveAPI, AWS CLI)

- Detective API : Utilisez l'`DeleteMembers`opération. Spécifiez le graphique ARN et la liste des identifiants de compte pour les comptes de membres à supprimer.
- AWS CLI: À l'invite de commande, exécutez la commande `delete-members`.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

Exemple :

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Python script

Detective fournit un script open source dans. GitHub Vous pouvez utiliser ce script pour supprimer une liste spécifique de comptes membres des graphes de comportement d'un compte administrateur dans une liste spécifiée de régions.

Pour plus d'informations sur la configuration et l'utilisation GitHub des scripts, consultezthe section called "Scripts Python d'Amazon Detective".

Pour les comptes membres : gestion des invitations des graphes de comportement et des appartenances

Amazon Detective facture à chaque compte membre les données ingérées pour chaque graphe de comportement auquel il contribue.

La page Gestion des comptes permet aux comptes membres de voir les comptes administrateurs pour les graphes de comportement dont ils sont membres.

Les comptes membres invités à consulter un graphe de comportement peuvent consulter leurs invitations et y répondre. Ils peuvent également supprimer leur compte du graphe de comportement.

Pour le graphe du comportement de l'organisation, les comptes d'organisation ne contrôlent pas si leur compte est un compte membre. Le compte administrateur Detective choisit les comptes de l'organisation à activer ou à désactiver en tant que comptes membres.

Table des matières

- IAMPolitique requise pour un compte de membre
- Afficher la liste de vos invitations à des graphes de comportement
- Réponse à une invitation de graphe de comportement
- Supprimer votre compte d'un graphe de comportement

IAMPolitique requise pour un compte de membre

Avant qu'un compte membre puisse consulter et gérer les invitations, la IAM politique requise doit être attachée à son principal. Le principal peut être un utilisateur ou un rôle existant, ou vous pouvez en créer un autre à utiliser pour Detective.

Idéalement, le compte administrateur demande à son IAM administrateur de joindre la politique requise.

La IAM politique relative aux comptes membres donne accès aux actions relatives aux comptes des membres dans Amazon Detective. L'invitation par e-mail à contribuer à un graphique de comportement inclut le texte de cette IAM politique.

Pour appliquer cette politique, remplacez-la *<behavior graph ARN>* par le graphiqueARN.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
```

```
        "detective:DisassociateMembership",
        "detective:RejectInvitation"
      ],
      "Resource": "<behavior graph ARN>"
    },
   {
    "Effect":"Allow",
    "Action":[
        "detective:BatchGetMembershipDatasources",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations"
    ],
    "Resource":"*"
   }
 ]
}
```

Notez que les comptes d'organisation figurant dans le graphe de comportement de l'organisation ne reçoivent pas d'invitations et ne peuvent pas dissocier leur compte du graphe du comportement de l'organisation. S'ils n'appartiennent pas à d'autres graphes de comportement, ils ont uniquement besoin de l'autorisation `ListInvitations`. `ListInvitations` leur permet de voir le compte administrateur du graphe de comportement. Les autorisations permettant de gérer les invitations et de dissocier les appartenances ne s'appliquent qu'aux appartenances sur invitation.

Afficher la liste de vos invitations à des graphes de comportement

Depuis la console Amazon DetectiveAPI, Detective ou AWS Command Line Interface un compte membre peut consulter ses invitations à un graphique de comportement.

Afficher les invitations à des graphes de comportement (console)

Vous pouvez consulter les invitations à créer des graphiques de comportement à partir du AWS Management Console.

Pour afficher les invitations à des graphes de comportement (console)

1. Connectez-vous au AWS Management Console. Ouvrez ensuite la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, choisissez Gestion des comptes.

Sur la page Gestion des comptes, la section Mes comptes administrateurs contient vos invitations à des graphes de comportement ouvertes et acceptées dans la région actuelle. Pour un compte d'organisation, Mes comptes administrateurs contient également le graphe du comportement de l'organisation.

Si votre compte est actuellement en période d'essai gratuit, la page affiche également le nombre de jours restants pour votre essai gratuit.

La liste ne contient pas les invitations que vous avez refusées, les appartenances que vous avez résiliées, ou les appartenances supprimées par le compte administrateur.

Chaque invitation indique le numéro de compte administrateur, la date à laquelle l'invitation a été acceptée et le statut actuel de l'invitation.

- Pour les invitations auxquelles vous n'avez pas répondu, le statut est Invité.
- Pour les invitations que vous avez acceptées, le statut est Activé ou Non activé.

  Si le statut est Activé, votre compte fournit des données au graphe de comportement.

  Si le statut est Non activé, votre compte ne fournit aucune donnée au graphe de comportement.

  Le statut de votre compte est initialement défini sur Non activé, tandis que Detective vérifie si vous l'avez GuardDuty activé et, dans l'affirmative, si votre compte est susceptible d'entraîner un dépassement du quota de Detective par le volume de données du graphique de comportement.

  Si votre compte n'entraîne pas un dépassement du quota par le graphe de comportement, Detective actualise le statut de votre compte en le définissant comme Activé. Dans le cas contraire, le statut reste Non activé.

  Lorsque le graphe de comportement est capable de s'adapter au volume de données de votre compte, Detective le met automatiquement à jour sur Activé. Par exemple, le compte administrateur peut supprimer d'autres comptes membres afin que le vôtre puisse être activé. Le compte administrateur peut également activer votre compte manuellement.

Afficher les invitations à des graphes de comportement (DetectiveAPI, AWS CLI)

Vous pouvez répertorier les invitations du Detective API ou du AWS Command Line Interface.

Pour récupérer une liste des invitations ouvertes et acceptées à des graphes comportementaux (DetectiveAPI, AWS CLI)

- Detective API : Utilisez l'`ListInvitations`opération.
- AWS CLI: À l'invite de commande, exécutez la commande `list-invitations`.

```
aws detective list-invitations
```

Réponse à une invitation de graphe de comportement

Une fois que vous avez accepté une invitation, Detective vérifie le nombre de comptes de membres. Le nombre maximum de comptes membres pour un graphe de comportement est de 1 200. Si votre graphe de comportement contient déjà 1 200 comptes membres, les nouveaux comptes ne peuvent pas être activés.

Une fois que vous avez accepté l'invitation, Detective est activé sur votre compte. Detective vérifie si votre volume de données est dans les limites du quota de Detective. Le volume de données entrant dans un graphe de comportement doit être inférieur au maximum autorisé par Detective. Si le volume actuellement ingéré est supérieur à la limite de 10 To par jour, vous ne pouvez pas ajouter d'autres comptes et Detective désactivera toute nouvelle ingestion de données. La console Detective affiche une notification indiquant que le volume de données est trop important et que le statut reste Non activé.

Si vous refusez l'invitation, elle est supprimée de votre liste d'invitations et Detective n'utilise pas les données de votre compte dans le graphe de comportement.

Réponse à une invitation de graphe de comportement (console)

Vous pouvez utiliser le AWS Management Console pour répondre à l'invitation par e-mail, qui inclut un lien vers la console Detective. Vous ne pouvez répondre qu'à une invitation dont le statut est Invité.

Pour répondre à une invitation de graphe de comportement (console)

1. Ouvrez la console Amazon Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, choisissez Gestion des comptes.
3. Sous Mes comptes administrateurs, choisissez Accepter l'invitation pour accepter l'invitation et commencer à ajouter des données au graphe de comportement.

Pour refuser l'invitation et la supprimer de la liste, choisissez Refuser.

Répondre à une invitation à un graphe de comportement (DetectiveAPI, AWS CLI)

Vous pouvez répondre aux invitations du Detective API ou du AWS Command Line Interface.

Pour accepter une invitation à un graphe comportemental (DetectiveAPI, AWS CLI)

- Detective API : Utilisez l'`AcceptInvitation`opération. Vous devez spécifier le graphiqueARN.
- AWS CLI: À l'invite de commande, exécutez la commande `accept-invitation`.

```
aws detective accept-invitation --graph-arn <behavior graph ARN>
```

Exemple :

```
aws detective accept-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Pour refuser une invitation à un graphe comportemental (DetectiveAPI, AWS CLI)

- Detective API : Utilisez l'`RejectInvitation`opération. Vous devez spécifier le graphiqueARN.
- AWS CLI: À l'invite de commande, exécutez la commande `reject-invitation`.

```
aws detective reject-invitation --graph-arn <behavior graph ARN>
```

Exemple :

```
aws detective reject-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Supprimer votre compte d'un graphe de comportement

Après avoir accepté une invitation, vous pouvez supprimer à tout moment votre compte d'un graphe de comportement. Lorsque vous supprimez votre compte d'un graphe de comportement, Amazon Detective arrête l'ingestion de données de votre compte dans le graphe de comportement. Les données existantes restent dans le graphe de comportement.

Seuls les comptes invités peuvent supprimer leur compte d'un graphe de comportement. Les comptes d'organisation ne peuvent pas supprimer leur compte du graphe de comportement de l'organisation.

Suppression de votre compte d'un graphe de comportement (console)

Vous pouvez utiliser le AWS Management Console pour supprimer votre compte d'un graphique de comportement.

Pour supprimer votre compte d'un graphe de comportement (console)

1. Ouvrez la console Amazon Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, choisissez Gestion des comptes.
3. Sous Mes comptes administrateurs, pour le graphe de comportement que vous souhaitez résilier, choisissez Résilier.

Supprimer votre compte d'un graphique de comportement (DetectiveAPI, AWS CLI)

Vous pouvez utiliser le Detective API ou le AWS Command Line Interface pour supprimer votre compte d'un graphique de comportement.

Pour supprimer votre compte d'un graphe de comportement (DetectiveAPI, AWS CLI)

- Detective API : Utilisez l'`DisassociateMembership`opération. Vous devez spécifier le graphiqueARN.
- AWS CLI: À l'invite de commande, exécutez la commande `disassociate-membership`.

```
aws detective disassociate-membership --graph-arn <behavior graph ARN>
```

Exemple :

```
aws detective disassociate-membership --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Effet des actions du compte sur les graphes de comportement

Ces actions ont les effets suivants sur les données et l'accès à Amazon Detective.

Detective désactivé

Lorsqu'un compte administrateur désactive Detective, voici ce qui se produit :

- Le graphe de comportement est supprimé.
- Detective arrête l'ingestion de données provenant du compte administrateur et des comptes membres pour ce graphe de comportement.

Le compte membre a été supprimé du graphe de comportement

Lorsqu'un compte membre est supprimé d'un graphe de comportement, Detective arrête l'ingestion des données de ce compte.

Les données existantes dans le graphe de comportement ne sont pas affectées.

Pour les comptes invités, le compte est supprimé de la liste Mes comptes membres.

Pour les comptes d'organisation figurant dans le graphe de comportement de l'organisation, le statut du compte passe à Pas un membre.

Le compte membre quitte l'organisation

Lorsqu'un compte membre quitte une organisation, voici ce qui se produit :

- Le compte est supprimé de la liste Mes comptes membres pour le graphe du comportement de l'organisation.
- Detective arrête l'ingestion des données de ce compte.

Les données existantes dans le graphe de comportement ne sont pas affectées.

AWS compte suspendu

Lorsqu'un compte administrateur est suspendu AWS, le compte perd l'autorisation de consulter le graphique de comportement dans Detective. Detective arrête l'ingestion des données dans le graphe de comportement.

Lorsqu'un compte membre est suspendu AWS, Detective arrête d'ingérer les données de ce compte.

Après 90 jours, le compte est soit résilié, soit réactivé. Lorsqu'un compte administrateur est réactivé, ses autorisations Detective sont restaurées. Detective reprend l'ingestion des données du compte. Lorsqu'un compte membre est réactivé, Detective reprend l'ingestion des données du compte.

AWS compte fermé

Lorsqu'un AWS compte est fermé, Detective répond à la fermeture comme suit.

- Pour un compte administrateur, Detective supprime le graphe de comportement.
- Pour un compte membre, Detective supprime le compte du graphe de comportement.

AWS conserve les données relatives à la politique du compte pendant 90 jours à compter de la date d'entrée en vigueur de la fermeture du compte administrateur. À la fin de la période de 90 jours, supprime AWS définitivement toutes les données relatives à la politique du compte.

- Pour conserver les résultats pendant plus de 90 jours, vous pouvez archiver les politiques. Vous pouvez également utiliser une action personnalisée avec une EventBridge règle pour stocker les résultats dans un compartiment S3.
- Tant que les données AWS de politique sont conservées, lorsque vous rouvrez le compte fermé, le compte est AWS réaffecté en tant qu'administrateur du service et récupère les données de politique de service relatives au compte.
- Pour plus d'informations, consultez Clôture d'un compte.

> **Important**
>
> Pour les clients des AWS GovCloud (US) régions :
>
> - Avant de clôturer votre compte, sauvegardez puis supprimez les ressources de votre compte. Vous n'aurez plus accès à ces informations après la clôture du compte.

Utilisation de scripts Detective Python pour gérer les comptes

Amazon Detective fournit un ensemble de scripts Python open source dans le GitHub référentiel amazon-detective-multiaccount-scripts. Les scripts nécessitent Python 3.

Vous pouvez les utiliser pour effectuer les tâches suivantes :

- Activer Detective pour un compte administrateur dans toutes les régions.

  Lorsque vous activez Detective, vous pouvez attribuer des valeurs de balise au graphe de comportement.
- Ajouter des comptes membres aux graphes de comportement d'un compte administrateur dans toutes les régions.
- Envoyer éventuellement des e-mails d'invitation aux comptes membres. Vous pouvez également configurer la demande afin qu'aucun e-mail d'invitation ne soit envoyé.
- Supprimer les comptes membres des graphes de comportement d'un compte administrateur dans toutes les régions.
- Désactiver Detective pour un compte administrateur dans toutes les régions. Lorsqu'un compte administrateur désactive Detective, le graphe de comportement du compte administrateur dans chaque région est désactivé.

Vue d'ensemble du script **`enableDetective.py`**

Le script `enableDetective.py` effectue les opérations suivantes :

1. Il active Detective pour un compte administrateur dans chaque région spécifiée, si Detective n'est pas déjà activé sur le compte administrateur dans cette région.

   Lorsque vous activez Detective, vous pouvez attribuer des valeurs de balise au graphe de comportement.
2. Il envoie éventuellement des invitations depuis le compte administrateur vers les comptes membres spécifiés pour chaque graphe de comportement.

   Les e-mails d'invitation utilisent le contenu du message par défaut et ne peuvent pas être personnalisés.

   Vous pouvez également configurer la demande afin qu'aucun e-mail d'invitation ne soit envoyé.
3. Accepte automatiquement les invitations pour les comptes membres.

   Comme le script accepte automatiquement les invitations, les comptes membres peuvent ignorer ces messages.

   Nous vous recommandons de contacter directement les comptes membres pour les informer que les invitations sont acceptées automatiquement.

Vue d'ensemble du script **disableDetective.py**

Le script `disableDetective.py` supprime les comptes membres spécifiés des graphes de comportement du compte administrateur dans les régions spécifiées.

Il fournit également une option permettant de désactiver Detective pour le compte administrateur dans les régions spécifiées.

Autorisations requises pour les scripts

Les scripts nécessitent un AWS rôle préexistant dans le compte administrateur et dans tous les comptes de membres que vous ajoutez ou supprimez.

> **Note**
>
> Le nom du rôle doit être le même dans tous les comptes.

IAMles meilleures pratiques recommandées en matière de politique consistent à utiliser les rôles les moins étendus. Pour exécuter le flux de travail du script consistant à créer un graphe, à créer des membres et à ajouter des membres au graphe, les autorisations requises sont les suivantes :

- détective : CreateGraph
- détective : CreateMembers
- détective : DeleteGraph
- détective : DeleteMembers
- détective : ListGraphs
- détective : ListMembers
- détective : AcceptInvitation

Relation d'approbation de rôle

La relation d'approbation de rôle doit permettre à votre instance ou à vos informations d'identification locales d'assumer le rôle.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<ACCOUNTID>:user/<USERNAME>"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Si vous ne disposez pas d'un rôle commun incluant les autorisations requises, vous devez créer un rôle avec au moins ces autorisations dans chaque compte membre. Vous devez également créer le rôle dans le compte administrateur.

Lorsque vous créez le rôle, veillez à exécuter les actions suivantes :

- Utilisez le même nom de rôle dans chaque compte.
- Ajoutez les autorisations requises ci-dessus (recommandé) ou sélectionnez la politique AmazonDetectiveFullAccessgérée.
- Ajoutez un bloc de relation de confiance entre les rôles, comme indiqué ci-dessus.

Pour automatiser ce processus, vous pouvez utiliser le `EnableDetective.yaml` AWS CloudFormation modèle. Comme le modèle ne crée que des ressources globales, il peut être exécuté dans n'importe quelle région.

Configuration de l'environnement d'exécution pour les scripts Python

Vous pouvez exécuter les scripts à partir d'une EC2 instance ou d'une machine locale.

Lancement et configuration d'une EC2 instance

L'une des options pour exécuter les scripts consiste à les exécuter à partir d'une EC2 instance.

Pour lancer et configurer une EC2 instance

1. Lancez une EC2 instance dans votre compte administrateur. Pour en savoir plus sur le lancement d'une EC2 instance, consultez Getting Started with Amazon EC2 Linux Instances dans le guide de EC2 l'utilisateur Amazon.

2. Associez à l'instance un IAM rôle doté des autorisations permettant à l'instance d'appeler `AssumeRole` depuis le compte administrateur.

   Si vous avez utilisé le `EnableDetective.yaml` AWS CloudFormation modèle, un rôle d'instance avec un profil nommé `EnableDetective` a été créé.

   Sinon, pour plus d'informations sur la création d'un rôle d'instance, consultez le billet de blog Remplacer ou attacher facilement un IAM rôle à une EC2 instance existante à l'aide de la EC2 console.
3. Installez le logiciel requis :

   - APT: `sudo apt-get -y install python3-pip python3 git`
   - RPM: `sudo yum -y install python3-pip python3 git`
   - Boto (version minimum 1.15) : `sudo pip install boto3`
4. Clonez le référentiel sur l'EC2instance.

```
git clone https://github.com/aws-samples/amazon-detective-multiaccount-scripts.git
```

Configuration d'une machine locale pour exécuter les scripts

Vous pouvez également exécuter les scripts à partir de votre ordinateur local.

Pour configurer une machine locale afin d'exécuter les scripts

1. Assurez-vous que vous avez configuré sur votre ordinateur local les informations d'identification de votre compte administrateur autorisé à appeler `AssumeRole`.
2. Installez le logiciel requis :

   - Python 3
   - Boto (version minimum 1.15)
   - GitHub scripts

Plateforme	Instructions de configuration
Windows	1. Installez Python 3 (https://www.python.org/downloads/windows/).

Plateforme	Instructions de configuration
	2. Ouvrir une invite de commande. 3. Pour installer Boto, exécutez : `pip install boto3` 4. Téléchargez le code source du script depuis GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts).
Mac	1. Installez Python 3 (https://www.python.org/downloads/mac-osx/). 2. Ouvrir une invite de commande. 3. Pour installer Boto, exécutez : `pip install boto3` 4. Téléchargez le code source du script depuis GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts).
Linux	1. Pour installer Python 3, exécutez l'une des commandes suivantes : • `sudo apt-get -y install install python3-pip python3 git` • `sudo yum install git python` 2. Pour installer Boto, exécutez : `sudo pip install boto3` 3. Clonez le code source du script à partir de https://github.com/aws-samples/amazon-detective-multiaccount-scripts.

Création d'une liste `.csv` de comptes membres à ajouter ou à supprimer

Pour identifier les comptes membres à ajouter ou à supprimer dans les graphes de comportement, vous fournissez un fichier `.csv` contenant la liste des comptes.

Répertoriez chaque compte sur une ligne distincte. Chaque entrée de compte de membre contient l'identifiant du AWS compte et l'adresse e-mail de l'utilisateur root du compte.

Consultez l'exemple suivant:

```
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Exécution d'**enableDetective.py**

Vous pouvez exécuter le `enableDetective.py` script à partir d'une EC2 instance ou de votre machine locale.

Pour exécuter **enableDetective.py**

1. Copiez le `.csv` fichier `amazon-detective-multiaccount-scripts` dans le répertoire de votre EC2 instance ou de votre machine locale.
2. Passez au répertoire `amazon-detective-multiaccount-scripts`.
3. Exécutez le script `enableDetective.py`.

   ```
   enableDetective.py --master_account administratorAccountID --assume_role roleName
    --input_file inputFileName --tags tagValueList --enabled_regions regionList  --
   disable_email
   ```

Lorsque vous exécutez le script, remplacez les valeurs suivantes :

administratorAccountID

L'ID de AWS compte du compte administrateur.

roleName

Nom du AWS rôle à assumer dans le compte administrateur et dans le compte de chaque membre.

inputFileName

Nom du fichier `.csv` contenant la liste des comptes membres à ajouter aux graphes de comportement du compte administrateur.

tagValueList

(Facultatif) Une liste de valeurs de balise séparées par des virgules à attribuer à un nouveau graphe de comportement.

Pour chaque valeur de balise, le format est *key*=*value*. Par exemple :

```
--tags Department=Finance,Geo=Americas
```

regionList

(Facultatif) Une liste de régions séparées par des virgules dans laquelle ajouter les comptes membres au graphe de comportement du compte administrateur. Par exemple :

```
--enabled_regions us-east-1,us-east-2,us-west-2
```

Detective n'est peut-être pas encore activé sur le compte administrateur dans une région. Dans ce cas, le script active Detective et crée un nouveau graphe de comportement pour le compte administrateur.

Si vous ne fournissez pas de liste de régions, le script agit dans toutes les régions prises en charge par Detective.

`--disable_email`

(Facultatif) S'il est inclus, Detective n'envoie pas d'e-mails d'invitation aux comptes membres.

Exécution d'**disableDetective.py**

Vous pouvez exécuter le `disableDetective.py` script à partir d'une EC2 instance ou de votre machine locale.

Pour exécuter **disableDetective.py**

1. Copiez le fichier `.csv` dans le répertoire `amazon-detective-multiaccount-scripts`.
2. Pour utiliser le fichier `.csv` afin de supprimer les comptes membres répertoriés des graphes de comportement du compte administrateur dans une liste spécifiée de régions, exécutez le script `disableDetective.py` comme suit :

   ```
   disabledetective.py --master_account administratorAccountID --assume_role roleName
    --input_file inputFileName --disabled_regions regionList
   ```
3. Pour désactiver Detective pour le compte administrateur dans toutes les régions, exécutez le script `disableDetective.py` avec l'indicateur `--delete-master`.

```
disabledetective.py --master_account administratorAccountID --assume_role roleName
 --input_file inputFileName --disabled_regions regionList --delete_master
```

Lorsque vous exécutez le script, remplacez les valeurs suivantes :

administratorAccountID

L'ID de AWS compte du compte administrateur.

roleName

Nom du AWS rôle à assumer dans le compte administrateur et dans le compte de chaque membre.

inputFileName

Nom du fichier `.csv` contenant la liste des comptes membres à supprimer des graphes de comportement du compte administrateur.

Vous devez fournir un fichier `.csv` même si vous désactivez Detective.

regionList

(Facultatif) Une liste de régions séparées par des virgules dans lesquelles effectuer l'une des opérations suivantes :

- Supprimez les comptes membres des graphes de comportement du compte administrateur.
- Si l'indicateur `--delete-master` est inclus, désactivez Detective.

Par exemple :

```
--disabled_regions us-east-1,us-east-2,us-west-2
```

Si vous ne fournissez pas de liste de régions, le script agit dans toutes les régions prises en charge par Detective.

Intégration d'Amazon Detective à Amazon Security Lake

Amazon Security Lake est un service de lac de données de sécurité entièrement géré. Vous pouvez utiliser Security Lake pour centraliser automatiquement les données de sécurité provenant des AWS environnements, des fournisseurs SaaS, des sources sur site, des sources cloud et des sources tierces dans un lac de données spécialement conçu et stocké dans votre compte. AWS Security Lake vous aide à analyser les données de sécurité, afin que vous puissiez mieux comprendre votre posture de sécurité dans l'ensemble de votre organisation. Avec Security Lake, vous pouvez également améliorer la protection des charges de travail, des applications et des données.

Amazon Detective s'intègre à Amazon Security Lake, ce qui signifie que vous pouvez interroger et récupérer les données de journal brutes stockées par Security Lake.

Grâce à cette intégration, vous pouvez collecter les journaux et les événements à partir des sources suivantes, prises en charge de manière native par Security Lake. Detective prend en charge jusqu'à la version source 2 (OCSF 1.1.0).

- AWS CloudTrail événements de gestion version 1.0 et versions ultérieures
- Amazon Virtual Private Cloud (Amazon VPC) Flow Logs version 1.0 et ultérieure
- Journal d'audit Amazon Elastic Kubernetes Service (Amazon EKS), version 2.0. — Pour utiliser les journaux d'audit Amazon EKS comme source, vous devez `ram:ListResources` ajouter des autorisations IAM. Pour plus de détails, voir Ajouter les autorisations IAM requises à votre compte.

Pour en savoir plus sur la façon dont Security Lake convertit automatiquement les journaux et les événements provenant de AWS services pris en charge de manière native vers le schéma OCSF, consultez le guide de l'utilisateur d'Amazon Security Lake.

Après avoir intégré Detective à Security Lake, Detective commence à extraire les journaux bruts de Security Lake relatifs aux événements AWS CloudTrail de gestion et aux journaux de flux Amazon VPC. Pour plus de détails, consultez Interrogation des journaux bruts.

Permettre l'intégration de Detective à Security Lake

Pour intégrer Detective à Security Lake, vous devez suivre les étapes suivantes.

1. Avant de commencer

Utilisez un compte de gestion Organizations et désignez un administrateur Security Lake délégué pour votre organisation. Assurez-vous que Security Lake est activé et vérifiez que Security Lake collecte les journaux et les événements à partir AWS CloudTrail des événements de gestion et des journaux de flux Amazon Virtual Private Cloud (Amazon VPC).

Conformément à l'architecture de référence de sécurité, Detective recommande d'utiliser un compte Log Archive et de ne pas utiliser de compte Security Tooling pour le déploiement de Security Lake.

2. Création d'un abonné à Security Lake

   Pour utiliser les journaux et les événements d'Amazon Security Lake, vous devez être abonné à Security Lake. Procédez comme suit pour accorder l'accès aux requêtes à un administrateur de compte Detective.

3. Ajouter les autorisations AWS Identity and Access Management (IAM) requises à votre identité IAM.

   - Ajoutez ces autorisations pour créer une intégration de Detective avec Security Lake :
     - Associez ces autorisations AWS Identity and Access Management (IAM) à votre identité IAM. Pour plus de détails, consultez la section Ajouter les autorisations IAM requises à votre compte.
     - Ajoutez cette politique IAM au principal IAM que vous prévoyez d'utiliser pour transmettre le rôle de AWS CloudFormation service. Pour plus de détails, consultez la section Ajouter des autorisations à votre IAM principal.
   - Si vous avez déjà intégré Detective à Security Lake, pour utiliser l'intégration, associez ces autorisations (IAM) à votre identité IAM. Pour plus de détails, consultez la section Ajouter les autorisations IAM requises à votre compte.

4. Accepter l'invitation Resource Share ARN et activer l'intégration

Utilisez le AWS CloudFormation modèle pour configurer les paramètres nécessaires à la création et à la gestion de l'accès aux requêtes pour les abonnés de Security Lake. Pour les étapes détaillées de création d'une pile, voir Création d'une pile à l'aide du AWS CloudFormation modèle. Une fois que vous avez fini de créer la pile, activez l'intégration.

Pour découvrir comment intégrer Amazon Detective à Amazon Security Lake à l'aide de la console Detective, regardez la vidéo suivante : Intégration d'Amazon Detective à Amazon Security Lake- How to Setup -->

Avant de commencer à intégrer Detective à Security Lake

Cette rubrique décrit les étapes préliminaires, telles que la délégation d'un administrateur Security Lake pour votre organisation, l'activation de Security Lake pour votre compte d'administrateur Detective et la vérification que Security Lake collecte les journaux et les événements.

Security Lake s'intègre AWS Organizations pour gérer la collecte de journaux sur plusieurs comptes d'une organisation. Pour utiliser Security Lake pour une organisation, votre compte AWS Organizations de gestion doit d'abord désigner un administrateur Security Lake délégué pour votre organisation. L'administrateur délégué de Security Lake doit ensuite activer Security Lake et activer la collecte des journaux et des événements pour les comptes des membres de l'organisation.

Avant d'intégrer Security Lake à Detective, assurez-vous que Security Lake est activé pour le compte administrateur Detective. Vous devez d'abord configurer les paramètres de votre lac de données et configurer la collecte des journaux en activant Security Lake à l'aide de la console Security Lake. Pour connaître les étapes détaillées relatives à l'activation de Security Lake, consultez Getting Started dans le guide de l'utilisateur d'Amazon Security Lake.

Vérifiez également que Security Lake collecte des journaux et des événements à partir des événements de AWS CloudTrail gestion et des journaux de flux Amazon Virtual Private Cloud (Amazon VPC). Pour plus d'informations sur la collecte de journaux dans Security Lake, consultez la section Collecte de données à partir de AWS services dans le guide de l'utilisateur d'Amazon Security Lake.

Étape 1 : Création d'un abonné Security Lake dans Detective

Cette rubrique explique comment utiliser la console Detective pour créer un abonné à Security Lake.

Pour utiliser les journaux et les événements d'Amazon Security Lake, vous devez être abonné à Security Lake. Un abonné peut interroger les données collectées par Security Lake et y accéder. Un abonné disposant d'un accès aux requêtes peut interroger AWS Lake Formation des tables directement dans un bucket Amazon Simple Storage Service (Amazon S3) en utilisant des services tels qu'Amazon Athena. Pour devenir abonné, l'administrateur de Security Lake doit vous fournir un accès abonné permettant d'interroger le lac de données. Pour plus d'informations sur la manière dont

l'administrateur procède, consultez Création d'un abonné avec accès aux requêtes dans le Guide de l'utilisateur d'Amazon Security Lake.

Suivez ces étapes pour créer un abonné Security Lake afin d'accorder l'accès aux requêtes à un compte administrateur Detective.

Pour créer un abonné Detective dans Security Lake

1. Ouvrez la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, choisissez Intégrations.
3. Dans le volet des abonnés de Security Lake, notez les valeurs de l'ID de compte et de l'ID externe.

   Demandez à l'administrateur de Security Lake de les utiliser IDs pour :

   - Créer automatiquement un abonné Detective dans Security Lake.
   - Configurer l'abonné afin qu'il ait accès aux requêtes.
   - Pour vous assurer que l'abonné aux requêtes Security Lake est créé avec les autorisations Lake Formation, sélectionnez Lake Formation comme méthode d'accès aux données dans la console Security Lake.

   Lorsque l'administrateur de Security Lake crée un abonné, Security Lake génère automatiquement un ARN de partage de ressources Amazon. Demandez à l'administrateur de vous envoyer cet ARN.
4. Entrez l'ARN de partage de ressources fourni par l'administrateur de Security Lake dans le volet des abonnés de Security Lake.
5. Après avoir reçu l'ARN du partage des ressources de la part de l'administrateur de Security Lake, saisissez-le dans le champ Resource Share ARN du volet des abonnés de Security Lake.

Étape 2 : Ajouter les autorisations IAM requises à votre compte dans Detective

Cette rubrique explique les détails de la politique d'autorisation AWS Identity and Access Management (IAM) que vous devez ajouter à votre identité IAM.

Pour activer l'intégration de Detective à Security Lake, vous devez associer la politique d'autorisation AWS Identity and Access Management (IAM) suivante à votre identité IAM.

Attachez au rôle les politiques en ligne suivantes. Remplacez `athena-results-bucket` par le nom de votre compartiment Amazon S3 si vous souhaitez utiliser votre propre compartiment Amazon S3 pour stocker les résultats des requêtes Athena. Si vous souhaitez que Detective génère automatiquement un compartiment Amazon S3 pour stocker le résultat des requêtes Athena, supprimez l'intégralité de `S3ObjectPermissions` de la politique IAM.

Si vous ne disposez pas des autorisations requises pour associer cette politique à votre identité IAM, contactez votre AWS administrateur. Si vous disposez des autorisations requises mais qu'un problème survient, consultez la section Résoudre les messages d'erreur liés au refus d'accès dans le guide de l'utilisateur IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3ObjectPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::<athena-results-bucket>",
        "arn:aws:s3:::<athena-results-bucket>/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables"
      ],
```

```
      "Resource": [
        "arn:aws:glue:*:<ACCOUNT ID>:database/amazon_security_lake*",
        "arn:aws:glue:*:<ACCOUNT ID>:table/amazon_security_lake*/
amazon_security_lake*",
        "arn:aws:glue:*:<ACCOUNT ID>:catalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:BatchGetQueryExecution",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "lakeformation:GetDataAccess",
        "ram:ListResources"
      ],
      "Resource": "*"
    },
    {
       "Effect": "Allow",
        "Action": [
          "ssm:GetParametersByPath"
        ],
        "Resource": [
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI"
        ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:GetTemplateSummary",
        "iam:ListRoles"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
```

```
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "securitylake.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Étape 3 : Acceptation de l'invitation Resource Share ARN

Cette rubrique explique les étapes à suivre pour accepter l'invitation Resource Share ARN à l'aide d'un AWS CloudFormation modèle, étape obligatoire avant d'activer l'intégration de Detective à Security Lake.

Pour accéder aux journaux des données brutes depuis Security Lake, vous devez accepter l'invitation de partage des ressources provenant du compte Security Lake créé par l'administrateur de Security Lake. Vous devez également disposer des autorisations AWS Lake Formation pour configurer le partage de tables entre comptes. En outre, vous devez créer un compartiment Amazon Simple Storage Service (Amazon S3) capable de recevoir les journaux des requêtes brutes.

À l'étape suivante, vous allez utiliser un AWS CloudFormation modèle pour créer une pile pour : accepter l'invitation Resource Share ARN, créer les AWS Glue crawler ressources requises et accorder des autorisations d' AWS Lake Formation administrateur.

Pour accepter l'invitation Resource Share ARN et activer l'intégration

1. Créez une nouvelle CloudFormation pile à l'aide du CloudFormation modèle. Pour en savoir plus, consultez Création d'une pile à l'aide du modèle AWS CloudFormation.
2. Après avoir créé la pile, choisissez Enable integration pour activer l'intégration de Detective avec Security Lake.

Création d'une pile à l'aide du modèle AWS CloudFormation

Detective fournit un AWS CloudFormation modèle que vous pouvez utiliser pour configurer les paramètres nécessaires à la création et à la gestion de l'accès aux requêtes pour les abonnés de Security Lake.

Étape 1 : créer un rôle AWS CloudFormation de service

Vous devez créer un rôle AWS CloudFormation de service pour créer une pile à l'aide du AWS CloudFormation modèle. Si vous ne disposez pas des autorisations requises pour créer un rôle de service, contactez l'administrateur du compte administrateur Detective. Pour plus d'informations sur le rôle de service AWS CloudFormation , consultez Rôle de service AWS CloudFormation.

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet de navigation de la console IAM, sélectionnez Roles (Rôles), puis Create role (Créer un rôle).
3. Pour Sélectionner une entité de confiance, choisissez Service AWS .
4. Sélectionnez AWS CloudFormation. Ensuite, choisissez Suivant.
5. Entrez un nom pour le rôle. Par exemple, `CFN-DetectiveSecurityLakeIntegration`.
6. Attachez au rôle les politiques en ligne suivantes. Remplacez `<Account ID>` par votre numéro de AWS compte.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CloudFormationPermission",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateChangeSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:aws:transform/*"
            ]
        },
        {
            "Sid": "IamPermissions",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:AttachRolePolicy",
                "iam:DetachRolePolicy",
                "iam:UpdateAssumeRolePolicy",
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy",
                "iam:CreatePolicy",
                "iam:DeletePolicy",
                "iam:PassRole",
                "iam:GetRole",
                "iam:GetRolePolicy"
            ],
            "Resource": [
                "arn:aws:iam::<ACCOUNT ID>:role/*",
                "arn:aws:iam::<ACCOUNT ID>:policy/*"
            ]
        },
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket*",
                "s3:PutBucket*",
                "s3:GetBucket*",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:GetEncryptionConfiguration"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "LambdaPermissions",
            "Effect": "Allow",
            "Action": [
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:GetFunction",
                "lambda:TagResource",
                "lambda:InvokeFunction"
```

```
            ],
            "Resource": [
                "arn:aws:lambda:*:<ACCOUNT ID>:function:*"
            ]
        },
        {
            "Sid": "CloudwatchPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:DeleteLogGroup",
                "logs:DescribeLogGroups"
            ],
            "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
        },
        {
            "Sid": "KmsPermission",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:*:<ACCOUNT ID>:key/*"
        }
    ]
}
```

Étape 2 : Ajouter des autorisations à votre principal IAM.

Vous aurez besoin des autorisations suivantes pour créer une pile à l'aide du rôle de CloudFormation service que vous avez créé à l'étape précédente. Ajoutez la politique IAM suivante au principal IAM que vous prévoyez d'utiliser pour transmettre le rôle de CloudFormation service. Vous utiliserez ce principal d'IAM pour créer la pile. Si vous ne disposez pas des autorisations requises pour ajouter la politique IAM, contactez l'administrateur du compte administrateur Detective.

> **Note**
>
> Dans la stratégie suivante, le terme `CFN-DetectiveSecurityLakeIntegration` utilisé dans cette stratégie fait référence au rôle que vous avez créé dans l'étape précédente du rôle de service `Creating an AWS CloudFormation`. Remplacez-le par le nom de rôle que vous avez saisi à l'étape précédente s'il est différent.

```
 {
    "Version": "2012-10-17",
    "Statement": [
        {
             "Sid": "PassRole",
             "Effect": "Allow",
             "Action":
             [
                "iam:GetRole",
                "iam:PassRole"
             ],
             "Resource": "arn:aws:iam::<ACCOUNT ID>:role/CFN-
DetectiveSecurityLakeIntegration"
        },
        {
            "Sid": "RestrictCloudFormationAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:UpdateStack"
            ],
            "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*",
            "Condition": {
                "StringEquals": {
                    "cloudformation:RoleArn": [
                        "arn:aws:iam::<ACCOUNT ID>:role/CFN-
DetectiveSecurityLakeIntegration"
                    ]
                }
            }
        },
        {
            "Sid": "CloudformationDescribeStack",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:GetStackPolicy"
            ],
            "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*"
        },
        {
```

```
            "Sid": "CloudformationListStacks",
            "Effect": "Allow",
            "Action": [
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:GetLogEvents"
            ],
            "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
        }
    ]
}
```

Étape 3 : Spécification de valeurs personnalisées dans la AWS CloudFormation console

1. Accédez à la AWS CloudFormation console depuis Detective.
2. (Facultatif) Saisissez un Nom de pile. Le nom de la pile est renseigné automatiquement. Vous pouvez remplacer le nom de la pile par un nom qui n'entre pas en conflit avec les noms de pile existants.
3. Entrez les Paramètres suivants.

   - AthenaResultsBucket— Si vous ne saisissez aucune valeur, ce modèle génère un compartiment Amazon S3. Si vous souhaitez utiliser votre propre compartiment, entrez un nom de compartiment pour stocker les résultats des requêtes Athena. Si vous utilisez votre propre compartiment, assurez-vous qu'il se trouve dans la même région que l'ARN du partage de ressources. Si vous utilisez votre propre compartiment, assurez-vous que le `LakeFormationPrincipals` que vous avez choisi est autorisé à y écrire des objets et à en lire. Pour plus d'informations sur les autorisations de compartiment, consultez Résultats des requêtes et requêtes récentes dans le Guide de l'utilisateur Amazon Athena.
   - DTRegion— Ce champ est prérempli. Ne modifiez pas les valeurs du champ.
   - LakeFormationPrincipals— Entrez l'ARN des principaux IAM (par exemple, l'ARN du rôle IAM) auxquels vous souhaitez accorder l'accès pour utiliser l'intégration Security Lake, séparés par des virgules. Il peut s'agir de vos analystes de sécurité et de vos ingénieurs de sécurité qui utilisent Detective.

Vous ne pouvez utiliser que les principals d'IAM auxquels vous avez précédemment attaché les autorisations IAM à l'étape [`Step 2: Add the required IAM permissions to your account`].

- ResourceShareARN — Ce champ est prérempli. Ne modifiez pas les valeurs du champ.

4. Autorisations

   Rôle IAM : sélectionnez le rôle IAM que vous avez créé à l'étape `Creating an AWS CloudFormation Service Role`. Vous pouvez éventuellement le laisser vide si votre rôle IAM en cours dispose de toutes les autorisations requises lors de l'étape `Creating an AWS CloudFormation Service Role`.

5. Passez en revue et cochez toutes les cases J'accepte, puis cliquez sur le bouton Créer une pile. Pour plus de détails, consultez les ressources IAM suivantes qui seront créées.

```
* ResourceShareAcceptorCustomResourceFunction
    - ResourceShareAcceptorLambdaRole
    - ResourceShareAcceptorLogsAccessPolicy
* SsmParametersCustomResourceFunction
    - SsmParametersLambdaRole
    - SsmParametersLogsAccessPolicy
* GlueDatabaseCustomResourceFunction
    - GlueDatabaseLambdaRole
    - GlueDatabaseLogsAccessPolicy
* GlueTablesCustomResourceFunction
    - GlueTablesLambdaRole
    - GlueTablesLogsAccessPolicy
```

Étape 4 : ajout de la politique de compartiment Amazon S3 aux principes IAM dans **`LakeFormationPrincipals`**

(Facultatif) Si vous laissez le modèle générer un `AthenaResultsBucket` à votre place, vous devez associer la politique suivante aux noms de principal IAM dans `LakeFormationPrincipals`.

```
{
  "Sid": "S3ObjectPermissions",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:PutObject"
```

```
  ],
  "Resource": [
    "arn:aws:s3:::<athena-results-bucket>",
    "arn:aws:s3:::<athena-results-bucket>/*"
  ]
}
```

Remplacez `athena-results-bucket` par le `AthenaResultsBucket` nom. `AthenaResultsBucket`Vous pouvez les trouver sur la AWS CloudFormation console :

1. Ouvrez la AWS CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation.
2. Cliquez sur votre pile.
3. Cliquez sur l'onglet Ressources.
4. Recherchez l'identifiant logique `AthenaResultsBucket` et copiez son identifiant physique.

Modification de la configuration de l'intégration de Detective

Si vous souhaitez modifier les paramètres que vous avez utilisés pour intégrer Detective à Security Lake, vous pouvez les modifier, puis réactiver l'intégration. Vous pouvez modifier le AWS CloudFormation modèle pour réactiver cette intégration dans les scénarios suivants :

- Pour mettre à jour l'abonnement Security Lake, vous pouvez créer un nouvel abonné ou l'administrateur de Security Lake peut mettre à jour la source de données de l'abonnement existant.
- Spécifier un compartiment Amazon S3 différent et y stocker les journaux des requêtes brutes.
- Pour spécifier les différents principaux Lake Formation.

Lorsque vous réactivez l'intégration de Detective à Security Lake, vous pouvez modifier le Resource Share ARN et consulter les autorisations IAM. Pour modifier les autorisations IAM, vous pouvez accéder à la console IAM depuis Detective. Vous pouvez également modifier les valeurs que vous avez saisies précédemment dans le AWS CloudFormation modèle. Vous devez supprimer la CloudFormation pile existante et la recréer pour réactiver l'intégration.

Pour réactiver l'intégration de Detective à Security Lake

1. Ouvrez la console Detective à l'adresse https://console.aws.amazon.com/detective/.

2. Dans le volet de navigation, choisissez Intégrations.
3. Vous pouvez modifier l'intégration en suivant l'une des étapes suivantes :

   - Dans le volet Security Lake, choisissez Modifier.
   - Dans le volet Security Lake, choisissez Afficher. Dans la page de la vue, choisissez Modifier.

4. Entrez un nouvel ARN de partage de ressources pour accéder aux sources de données d'une région.
5. Consultez les autorisations IAM en cours et accédez à la console IAM si vous souhaitez modifier les autorisations IAM.
6. Modifiez les valeurs du CloudFormation modèle.

   1. Supprimez d'abord la pile existante, avant d'en créer une nouvelle. Si vous ne supprimez pas la pile existante et que vous essayez d'en créer une nouvelle dans la même région, votre demande échoue. Pour en savoir plus, consultez Supprimer une CloudFormation pile.

   1. Créez une nouvelle CloudFormation pile. Pour en savoir plus, consultez Création d'une pile à l'aide du modèle AWS CloudFormation.

7. Choisissez Activer l'intégration.

AWS Régions prises en charge pour l'intégration de Detective à Security Lake

Vous pouvez intégrer Detective à Security Lake dans les AWS régions suivantes.

Nom de la région	Région	Point de terminaison	Protocole ;
USA Est (Ohio)	us-east-2	securitylake.us-east-2.amazonaws.com	HTTPS
USA Est (Virginie du Nord)	us-east-1	securitylake.us-east-1.amazonaws.com	HTTPS
USA Ouest (Californie du Nord)	us-west-1	securitylake.us-west-1.amazonaws.com	HTTPS

Nom de la région	Région	Point de terminaison	Protocole ;
USA Ouest (Oregon)	us-west-2	securitylake.us-west-2.amazonaws.com	HTTPS
Asie-Pacifique (Mumbai)	ap-south-1	securitylake.ap-south-1.amazonaws.com	HTTPS
Asie-Pacifique (Séoul)	ap-northeast-2	securitylake.ap-northeast-2.amazonaws.com	HTTPS
Asie-Pacifique (Singapour)	ap-southeast-1	securitylake.ap-southeast-1.amazonaws.com	HTTPS
Asie-Pacifique (Sydney)	ap-southeast-2	securitylake.ap-southeast-2.amazonaws.com	HTTPS
Asie-Pacifique (Tokyo)	ap-northeast-1	securitylake.ap-northeast-1.amazonaws.com	HTTPS
Canada (Centre)	ca-central-1	securitylake.ca-central-1.amazonaws.com	HTTPS
Europe (Francfort)	eu-central-1	securitylake.eu-central-1.amazonaws.com	HTTPS
Europe (Irlande)	eu-west-1	securitylake.eu-west-1.amazonaws.com	HTTPS
Europe (Londres)	eu-west-2	securitylake.eu-west-2.amazonaws.com	HTTPS
Europe (Paris)	eu-west-3	securitylake.eu-west-3.amazonaws.com	HTTPS
Europe (Stockholm)	eu-north-1	securitylake.eu-north-1.amazonaws.com	HTTPS
Amérique du Sud (São Paulo)	sa-east-1	securitylake.sa-east-1.amazonaws.com	HTTPS

Interrogation des journaux bruts dans Detective

Après avoir intégré Detective à Security Lake, Detective commence à extraire les journaux bruts de Security Lake relatifs aux événements de AWS CloudTrail gestion et aux journaux de flux Amazon Virtual Private Cloud (Amazon VPC).

> **Note**
>
> L'interrogation des journaux bruts dans Detective n'entraîne pas de frais supplémentaires. Les frais d'utilisation des autres AWS services, y compris Amazon Athena, s'appliquent toujours aux tarifs publiés.

AWS CloudTrail des événements de gestion sont disponibles pour les profils suivants :

- AWS compte
- AWS utilisateur
- AWS rôle
- AWS Session de rôle
- EC2 Instance Amazon
- Compartiment Amazon S3
- Adresse IP
- Cluster Kubernetes
- Module Kubernets
- Sujet Kubernets
- Rôle IAM
- Séance de rôle IAM
- Utilisateur IAM

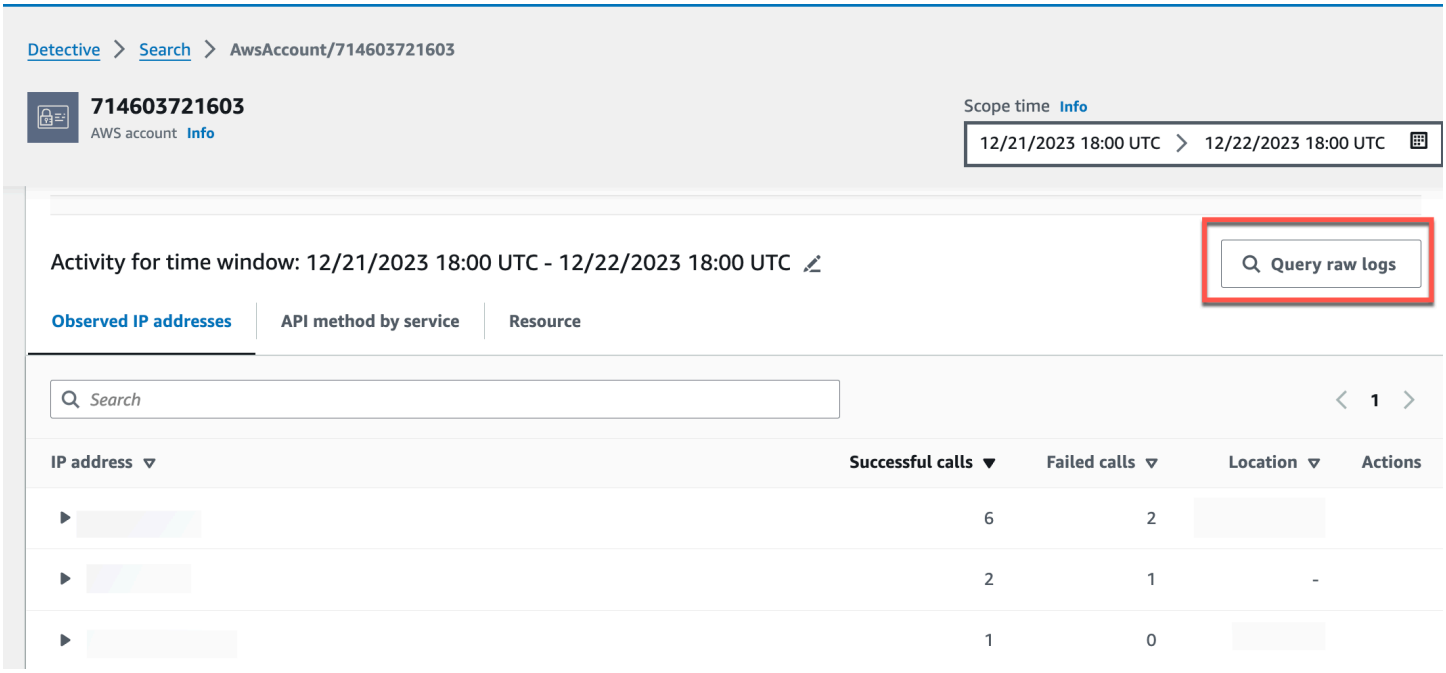
Les FLow journaux Amazon VPC sont disponibles pour les profils suivants :

- EC2 Instance Amazon
- Pod Kubernetes

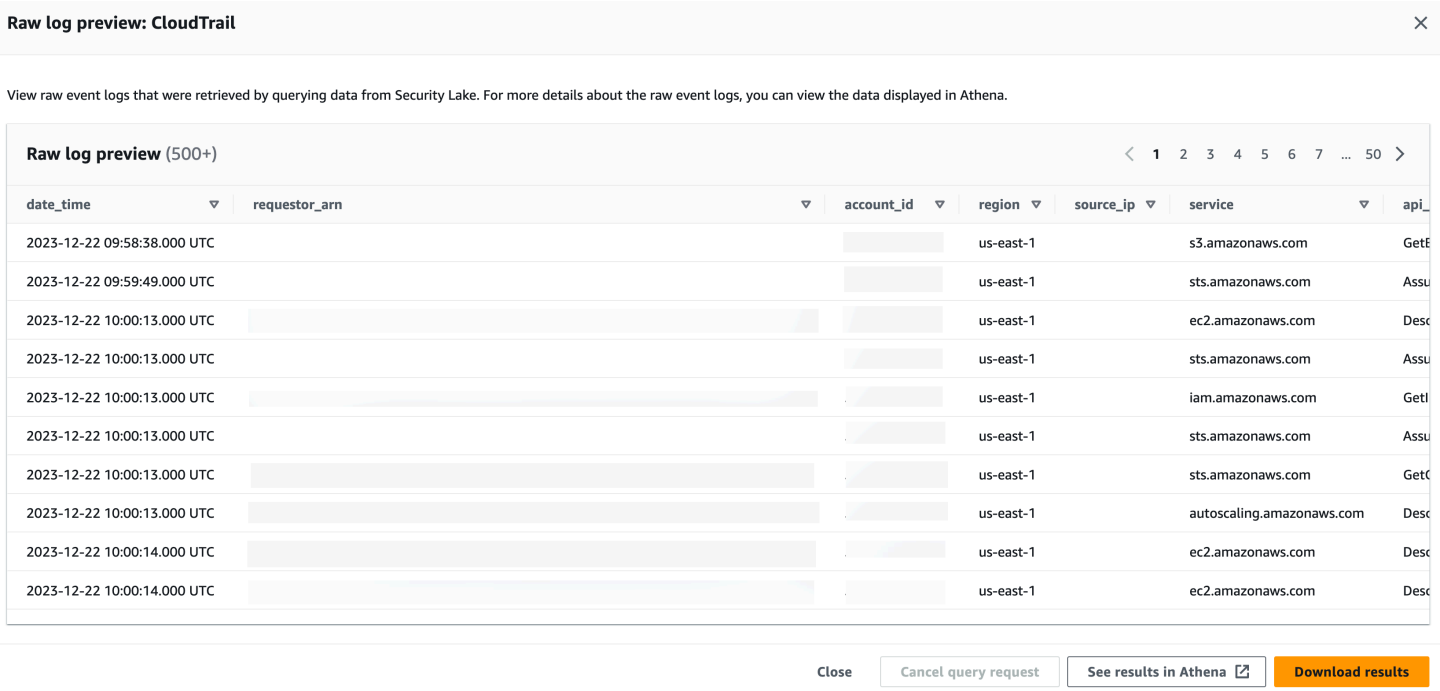
Pour découvrir comment intégrer Amazon Detective à Amazon Security Lake à l'aide de la console Detective, regardez la vidéo suivante : Intégration d'Amazon Detective à Amazon Security Lake- How to Use -->

Pour interroger les journaux bruts d'un compte AWS

1. Ouvrez la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, choisissez Rechercher, puis recherchez une `AWS account`.
3. Dans la section Volume global des appels d'API, choisissez Afficher les détails pour la durée de la portée.
4. À partir de là, vous pouvez commencer à interroger les journaux bruts.



Dans le tableau d'aperçu des journaux bruts, vous pouvez consulter les journaux et les événements extraits en interrogeant les données de Security Lake. Pour plus de détails sur les journaux d'événements bruts, vous pouvez consulter les données affichées dans Amazon Athena.



Dans le tableau d'interrogation des journaux bruts, vous pouvez annuler la demande de requête, afficher les résultats dans Amazon Athena et télécharger les résultats sous la forme d'un fichier de valeurs séparées par des virgules (.csv).

Si vous voyez des journaux dans Detective, mais que la requête n'a renvoyé aucun résultat, les raisons peuvent en être les suivantes.

- Les journaux bruts peuvent être disponibles dans Detective avant d'apparaître dans les tableaux des journaux de Security Lake. Réessayez ultérieurement.
- Les journaux peuvent ne pas être présents dans Security Lake. Si vous avez attendu pendant une longue période, cela indique que les journaux sont absents de Security Lake. Contactez votre administrateur Security Lake pour résoudre le problème.

Exemples

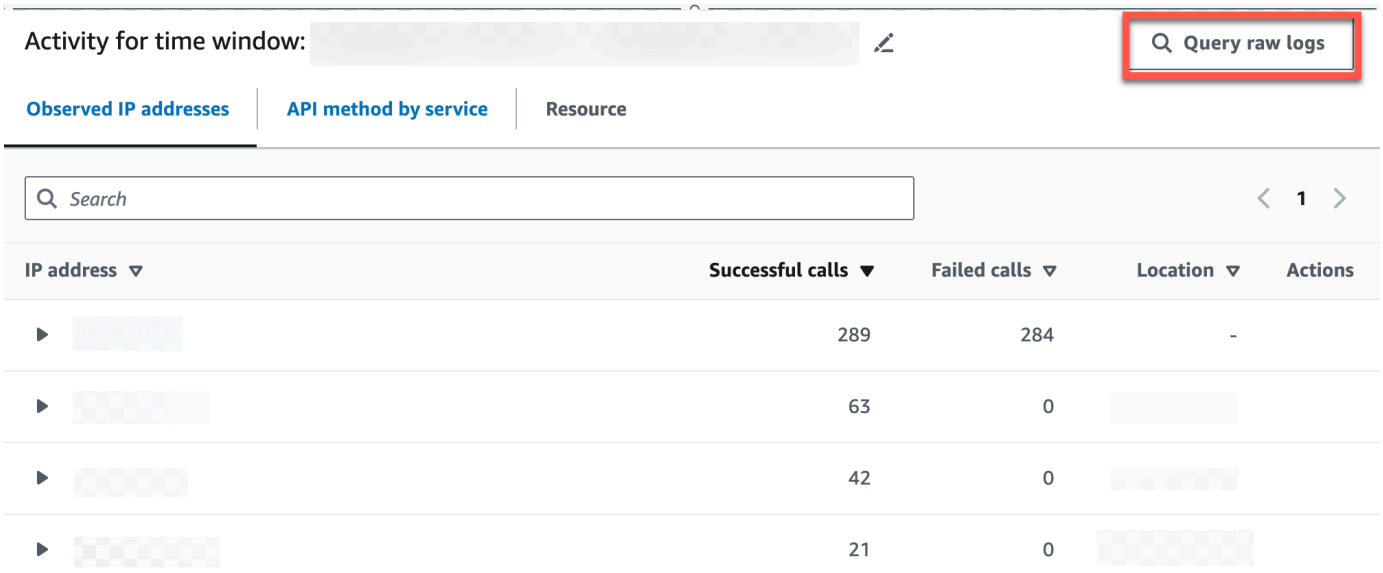
- Interrogation de logs bruts pour un rôle AWS
- Interrogation de journaux bruts pour un cluster Amazon EKS
- Interrogation de logs bruts pour une instance Amazon EC2

Interrogation de logs bruts pour un rôle AWS

Si vous souhaitez comprendre l'activité d'un AWS rôle dans une nouvelle géolocalisation, vous pouvez le faire dans la console Detective.

Pour interroger les journaux bruts d'un rôle AWS

1. Ouvrez la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Sur la page Detective Summary, dans la section « Géolocalisations récemment observées », notez le AWS rôle.
3. Dans le volet de navigation, choisissez Rôles, puis recherchez le `AWS role`.
4. Pour le AWS rôle, développez la ressource pour afficher les appels d'API spécifiques émis par cette ressource à partir de cette adresse IP.
5. Choisissez l'icône en forme de loupe à côté de l'appel d'API que vous souhaitez étudier pour ouvrir le tableau d'aperçu des journaux bruts.



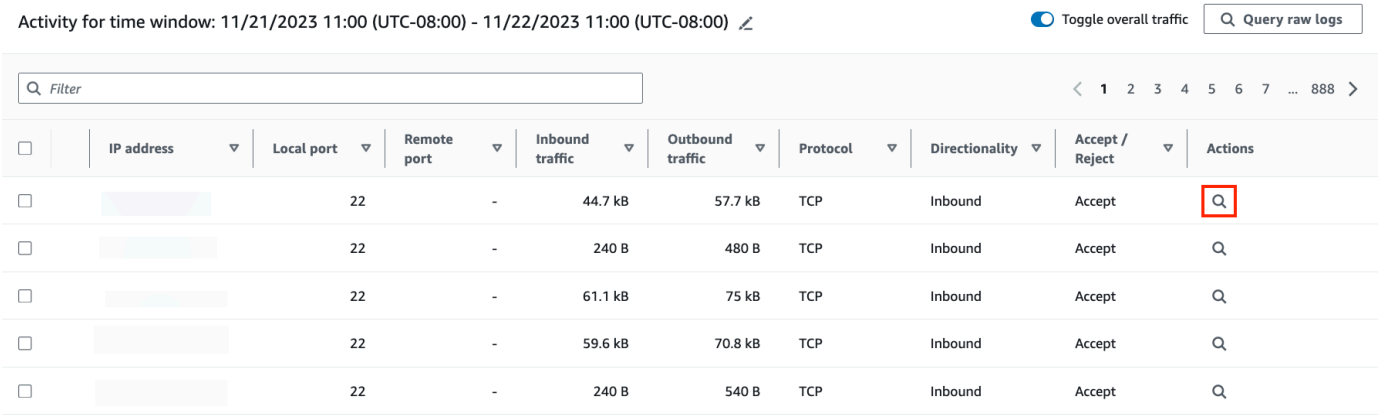
Interrogation de journaux bruts pour un cluster Amazon EKS

1. Ouvrez la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Sur la page Detective Summary, section Clusters de conteneurs contenant le plus grand nombre de pods créés, accédez à un cluster Amazon EKS.
3. Sur la page de détails du cluster Amazon EKS, sélectionnez l'onglet Activité de l'API Kubernets.

4. Dans la section Activité globale de l'API Kubernets impliquant ce cluster Amazon EKS, choisissez les détails d'affichage pour la durée du champ d'application.
5. À partir de là, vous pouvez commencer à interroger les journaux bruts.

Interrogation de logs bruts pour une instance Amazon EC2

1. Ouvrez la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, choisissez Rechercher, puis recherchez une `Amazon EC2 instance`.
3. Dans la section Volume global des flux VPC, choisissez l'icône en forme de loupe à côté de l'appel d'API que vous souhaitez étudier pour ouvrir le tableau d'aperçu des journaux bruts.
4. À partir de là, vous pouvez commencer à interroger les journaux bruts.



Dans le tableau d'aperçu des journaux bruts, vous pouvez consulter les journaux et les événements extraits en interrogeant les données de Security Lake. Pour plus de détails sur les journaux d'événements bruts, vous pouvez consulter les données affichées dans Amazon Athena.

Dans le tableau d'interrogation des journaux bruts, vous pouvez annuler la demande de requête, afficher les résultats dans Amazon Athena et télécharger les résultats sous la forme d'un fichier de valeurs séparées par des virgules (.csv).

Désactivation de l'intégration de Detective à Security Lake

Si vous désactivez l'intégration de Detective à Security Lake, vous ne pouvez plus interroger les données des journaux et des événements depuis Security Lake.

Pour désactiver l'intégration de Detective à Security Lake

1. Ouvrez la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, choisissez Intégrations.
3. Supprimez la pile existante. Pour en savoir plus, consultez Supprimer une CloudFormation pile.
4. Dans le volet Désactivation de l'intégration à Security Lake, choisissez Désactiver.

Supprimer une CloudFormation pile

Si vous ne supprimez pas la pile existante, la création d'une nouvelle pile dans la même région échouera. Vous pouvez supprimer une CloudFormation pile à l'aide de la CloudFormation console ou de la AWS CLI.

Pour supprimer la AWS CloudFormation pile (console)

1. Ouvrez la AWS CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation.
2. Sur la page Stacks de la CloudFormation console, sélectionnez la pile que vous souhaitez supprimer. La pile doit être en cours d'exécution.
3. Dans le volet des détails de la pile, choisissez Supprimer.
4. Sélectionnez Supprimer la pile lorsque vous y êtes invité.

> **Note**
>
> L'opération de suppression de pile ne peut pas être arrêtée une fois qu'elle a commencé. La pile passe à l'état `DELETE_IN_PROGRESS`.

Une fois que la suppression est terminée, la pile indique l'état `DELETE_COMPLETE`.

Résolution des erreurs de suppression de pile

Si le message affiche une erreur d'autorisation `Failed to delete stack` après avoir cliqué sur le `Delete` bouton, cela signifie que votre rôle IAM n'est pas CloudFormation autorisé à supprimer une pile. Contactez l'administrateur de votre compte pour supprimer la pile.

Pour supprimer la CloudFormation pile (AWS CLI)

Entrez la commande suivante dans l'interface AWS CLI :

```
aws cloudformation delete-stack --stack-name your-stack-name --role-arn
      arn:aws:iam::<ACCOUNT ID>:role/CFN-DetectiveSecurityLakeIntegration
```

`CFN-DetectiveSecurityLakeIntegration` désigne la fonction du service créée à l'étape `Creating an AWS CloudFormation Service Role`.

Prévision et surveillance des coûts de Detective

Pour vous aider à suivre votre activité de Detective, la page Utilisation indique la quantité de données ingérées et le coût prévu.

- Pour les comptes administrateurs, la page Utilisation indique le volume de données et le coût prévu sur l'ensemble du graphe de comportement.
- Pour les comptes membres, la page Utilisation indique le volume de données et le coût prévu pour leur compte sur les graphes de comportement auxquels ils contribuent.

Detective prend également en charge la AWS CloudTrail journalisation.

Table des matières

- À propos de la version d'essai gratuite des graphes de comportement
- Surveillance de l'utilisation d'un compte administrateur Detective
- Surveillance de l'utilisation d'un compte de membre Detective
- Comment Amazon Detective calcule le coût prévisionnel

À propos de la version d'essai gratuite des graphes de comportement

Amazon Detective propose un essai gratuit de 30 jours pour chaque compte dans chaque région. L'essai gratuit d'un compte commence la première fois que l'une des actions suivantes se produit.

- Un compte active Detective manuellement et devient le compte administrateur d'un graphe de comportement.
- Un compte est désigné comme compte d'administrateur Detective pour une organisation dans AWS Organizations, et Detective est activé pour la première fois dans ce compte.
- Si Detective était déjà activé sur le compte administrateur du compte Detective avant sa désignation, le compte ne démarre pas un nouvel essai gratuit de 30 jours.
- Un compte accepte une invitation à devenir membre dans un graphe de comportement, et il est activé en tant que compte membre.
- Un compte d'organisation est activé en tant que compte membre par le compte administrateur Detective.

L'essai gratuit dure 30 jours à partir de ce moment. Le compte n'est pas facturé pour les données traitées pendant cette période. À la fin de la période d'essai, Detective commence à facturer au compte les données qu'il fournit aux graphes de comportement. Pour plus d'informations sur la manière dont vous pouvez suivre votre activité Detective, surveiller l'utilisation et consulter le coût prévisionnel, consultez Prévision et surveillance des coûts de Detective. Pour plus d'informations sur la tarification, consultez Tarification Detective

La même période de 30 jours est utilisée pour tous les graphes de comportement de la région. Par exemple, un compte est activé en tant que compte membre pour un graphe de comportement. Cela commence l'essai gratuit de 30 jours. Après 10 jours, le compte est activé pour un deuxième graphe de comportement dans la même région. Pour le deuxième graphe de comportement, le compte reçoit 20 jours de données gratuites.

L'essai gratuit offre de nombreux avantages :

- Les comptes administrateurs peuvent explorer les fonctionnalités de Detective pour vérifier sa valeur.
- Les comptes administrateurs et membres peuvent surveiller la quantité de données et le coût estimé avant que Detective ne commence à les facturer. Consultez the section called "Utilisation et coûts du compte administrateur" et the section called "Suivi de l'utilisation du compte membre".

Essai gratuit pour les sources de données facultatives

Detective propose également un essai gratuit de 30 jours pour les sources de données facultatives. Cet essai gratuit est distinct de l'essai gratuit fourni pour les principales sources de données Detective lorsque Detective est activé pour la première fois.

> **Note**
>
> Si un client désactive un package de source de données facultatif dans les 7 jours suivant son activation, Detective réinitialise automatiquement l'essai gratuit pour ce package de source de données s'il est de nouveau activé.

Pour activer ou désactiver une source de données facultative, consultez Types de sources de données facultatives dans Detective.

Surveillance de l'utilisation d'un compte administrateur Detective

Amazon Detective facture à chaque compte les données utilisées dans chaque graphe de comportement auquel le compte appartient. Detective facture un forfait échelonné par Go pour toutes les données, quelle que soit leur source.

Pour les comptes administrateurs, la page Utilisation de la console Detective vous permet de visualiser le volume de données ingérées par source de données ou par compte au cours des 30 derniers jours. Les comptes administrateurs voient également un coût prévisionnel pour une période typique de 30 jours pour leur compte et pour l'ensemble du graphe de comportement.

Pour consulter les informations d'utilisation de Detective

1. Connectez-vous au AWS Management Console. Ouvrez ensuite la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, sous Paramètres, choisissez Utilisation.
3. Choisissez un onglet pour choisir entre l'affichage d'utilisation par source de données ou par compte.

Volume de données ingérées pour chaque compte

Le volume ingéré par compte membre répertorie les comptes actifs dans le graphe de comportement. Il ne répertorie pas les comptes des membres qui ont été supprimés.

Pour chaque compte, la liste des volumes ingérés fournit les informations suivantes.

- L'identifiant du AWS compte et l'adresse e-mail de l'utilisateur root.
- Date à laquelle le compte a commencé à fournir des données au graphe de comportement.

  Pour le compte administrateur, il s'agit de la date à laquelle le compte a activé Detective.

  Pour les comptes membres, il s'agit de la date à laquelle un compte a été activé en tant que compte membre après avoir accepté l'invitation.
- Volume de données ingérées depuis le compte du membre au cours des 30 derniers jours. Le total inclut tous les types de sources.
- Si le compte est actuellement en période d'essai gratuit. Pour les comptes qui sont actuellement en période d'essai gratuit, la liste indique le nombre de jours restants.

Si aucun des comptes n'est en période d'essai gratuit, la colonne d'état de l'essai gratuit ne s'affiche pas.

Coûts prévus pour le graphe de comportement

Le coût prévisionnel de ce compte indique le coût prévisionnel pour 30 jours de données pour le compte administrateur. Le coût prévisionnel est basé sur le volume moyen quotidien du compte membre.

> **Important**
>
> Ce montant est uniquement un coût prévisionnel. Il projette le coût total des données du compte administrateur pour une période typique de 30 jours. Il est basé sur l'utilisation des 30 derniers jours. Consultez the section called "Comment Amazon Detective calcule le coût prévisionnel".

Coût prévu pour le graphe de comportement

Le coût prévisionnel de tous les comptes indique le coût total prévu pour 30 jours de données pour l'ensemble du graphe de comportement. Le coût prévisionnel est basé sur le volume moyen quotidien du compte.

> **Important**
>
> Ce montant est uniquement un coût prévisionnel. Il projette le coût total des données du graphe de comportement pour une période typique de 30 jours. Il est basé sur l'utilisation des 30 derniers jours. Le coût prévu n'inclut pas les comptes membres qui ont été supprimés du graphe de comportement. Consultez the section called "Comment Amazon Detective calcule le coût prévisionnel".

Volume de données ingérées par les packages sources

Sélectionnez Par package source pour afficher le volume de données ingérées répertorié par les différents packages source activés dans votre graphe de comportement.

Tous les comptes peuvent consulter ces données pour leurs propres comptes. Un compte administrateur peut voir des volets supplémentaires qui répertorient l'utilisation par package source pour chaque membre. Il ne répertorie pas les comptes des membres qui ont été supprimés.

Données clés Detective

Les panneaux Detective Core indiquent le volume de données ingérées à partir des sources principales de Detective (CloudTrail journaux, journaux de VPC flux et GuardDuty résultats) au cours des 30 derniers jours.

EKS journaux d'audit

EKSles panneaux de journaux d'audit indiquent le volume de données ingérées à partir des sources des journaux EKS d'audit au cours des 30 derniers jours. Les panneaux de ce package source ne sont disponibles que si les journaux EKS d'audit sont activés pour votre graphe de comportement.

Surveillance de l'utilisation d'un compte de membre Detective

Amazon Detective facture à chaque compte les données utilisées dans chaque graphe de comportement auquel le compte appartient. Detective facture un forfait échelonné par Go pour toutes les données, quelle que soit leur source.

Pour les comptes membres, la page Utilisation indique le volume de données et le coût prévu sur 30 jours pour ce compte uniquement.

Pour consulter les informations d'utilisation de Detective

1. Connectez-vous au AWS Management Console. Ouvrez ensuite la console Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, sous Paramètres, choisissez Utilisation.

Volume ingéré pour chaque graphe de comportement

Le volume ingéré de ce compte répertorie les graphes de comportement auxquels contribue le compte membre. Cela n'inclut pas les adhésions que vous avez résiliées, ni les adhésions supprimées par le compte administrateur.

Pour chaque graphe de comportement comprend des informations sur les points suivants :

- Nombre de compte pour le compte administrateur
- Volume de données ingérées depuis le compte membre au cours des 30 derniers jours. Le total inclut tous les types de sources.
- Date à laquelle le compte membre a été activé pour le graphe de comportement.

Coût projeté sur la base de graphes de comportement

Le coût prévisionnel de ce compte indique le coût prévu pour 30 jours de données pour le compte membre sur tous les graphes de comportement auxquels il contribue. Le coût prévisionnel est basé sur le volume moyen quotidien du compte membre.

> **Important**
>
> Ce montant est uniquement un coût prévisionnel. Il projette le coût total des données du compte administrateur pour une période typique de 30 jours. Il est basé sur l'utilisation des 30 derniers jours. Consultez the section called "Comment Amazon Detective calcule le coût prévisionnel".

Comment Amazon Detective calcule le coût prévisionnel

Pour calculer les valeurs de coût prévisionnelles affichées sur la page Utilisation, Detective effectue les opérations suivantes.

1. Pour obtenir le coût prévisionnel d'un compte individuel dans un graphe de comportement, Detective effectue les opérations suivantes.
   a. Calcule le volume moyen par jour. Il ajoute le volume de données pour tous les jours actifs, puis le divise par le nombre de jours pendant lesquels le compte a été actif.

      Si le compte a été activé il y a plus de 30 jours, le nombre de jours est de 30. Si le compte a été activé il y a moins de 30 jours, il s'agit du nombre de jours écoulés depuis la date d'acceptation.

      Par exemple, si le compte a été activé il y a 12 jours, Detective ajoute le volume ingéré pendant ces 12 jours, puis le divise par 12.

   b. Multiplie la moyenne quotidienne du compte par 30. Il s'agit de l'utilisation prévue du compte sur 30 jours.

   c. Utilise son modèle de tarification pour calculer le coût prévu sur 30 jours pour l'utilisation prévue sur 30 jours.
2. Pour obtenir le coût prévisionnel d'un compte individuel dans un graphe de comportement, Detective effectue les opérations suivantes :
   a. Combine l'utilisation prévue sur 30 jours de tous les comptes dans le graphe de comportement.
   b. Utilise son modèle de tarification pour calculer le coût prévu sur 30 jours pour l'utilisation totale prévue sur 30 jours.
3. Pour obtenir le coût prévisionnel d'un compte individuel dans un graphe de comportement, Detective effectue les opérations suivantes :
   a. Combine l'utilisation prévue sur 30 jours sur tous les graphes de comportement.
   b. Utilise son modèle de tarification pour calculer le coût prévu sur 30 jours pour l'utilisation totale prévue sur 30 jours.
4. Si vous utilisez un Amazon VPC partagé, Detective calcule le coût prévisionnel en fonction de l'activité de surveillance. Nous vous recommandons de revoir le coût prévisionnel de vos enquêtes en fonction de votre environnement.
   a. Si un compte membre Detective possède un Amazon VPC partagé et que d'autres comptes non Detective l'utilisent, Detective surveillera tout le trafic provenant de ce VPC. L'utilisation et les coûts augmenteront, et Detective fournira une visualisation de l'ensemble du flux de trafic au sein du VPC.
   b. Si vous disposez d'une instance EC2 au sein d'un Amazon VPC partagé et que le propriétaire du VPC partagé n'est pas membre de Detective, Detective ne surveillera aucun trafic provenant du VPC. Par conséquent, l'utilisation et les coûts diminueront. Si vous souhaitez visualiser le flux de trafic au sein du VPC, vous devez ajouter le propriétaire de l'Amazon VPC en tant que membre de votre graphique Detective.

Sécurité dans Amazon Detective

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité.

  Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformitéAWS.

  Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Detective, consultez Services AWS concernés par le programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Detective. Les rubriques suivantes expliquent comment configurer Detective pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources de Detective.

Table des matières

- Protection des données dans Amazon Detective
- Gestion des identités et des accès pour Amazon Detective
- Validation de la conformité pour Amazon Detective
- Résilience dans Amazon Detective
- Sécurité de l'infrastructure dans Amazon Detective
- Bonnes pratiques en matière de sécurité pour Detective

Protection des données dans Amazon Detective

Le AWS modèle de responsabilité partagée modèle de de s'applique à la protection des données dans Amazon Detective. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. Il vous incombe de garder le contrôle sur votre contenu hébergé sur cette infrastructure. Vous êtes également responsable de la configuration de la sécurité et des tâches de gestion pour Services AWS que tu utilises. Pour plus d'informations sur la confidentialité des données, consultez la section Confidentialité des données FAQ. Pour plus d'informations sur la protection des données en Europe, consultez le AWS Modèle de responsabilité partagée et article de GDPR blog sur le AWS Blog sur la sécurité.

Pour des raisons de protection des données, nous vous recommandons de protéger Compte AWS informations d'identification et configuration des utilisateurs individuels avec AWS IAM Identity Center or 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) pour chaque compte.
- UtilisezSSL/TLSpour communiquer avec AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et enregistrement de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation CloudTrail des sentiers pour capturer AWS activités, voir Travailler avec les CloudTrail sentiers dans le AWS CloudTrail Guide de l'utilisateur.
- Utiliser AWS solutions de chiffrement, ainsi que tous les contrôles de sécurité par défaut intégrés 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 FIPS 140 à 3 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou unAPI, utilisez un FIPS point de terminaison. Pour plus d'informations sur les FIPS points de terminaison disponibles, voir Federal Information Processing Standard (FIPS) 140-3.

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 Detective ou un autre Services AWS à l'aide de la consoleAPI, AWS CLI, ou AWS SDKs. Toutes les données que vous entrez dans des

balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez un URL à un serveur externe, nous vous recommandons vivement de ne pas inclure d'informations d'identification dans le URL afin de valider votre demande auprès de ce serveur.

Detective chiffre toutes les données qu'il traite et stocke, tant au repos qu'en transit.

Table des matières

- Gestion des clés pour Amazon Detective

Gestion des clés pour Amazon Detective

Detective ne stockant aucune donnée client personnellement identifiable, il utilise Clés gérées par AWS.

Ce type de clé KMS peut être utilisé sur plusieurs comptes. Consultez la description des clés AWS détenues dans le guide du AWS Key Management Service développeur.

Ce type de clé KMS effectue automatiquement une rotation chaque année (environ 365 jours). Consultez la description de la rotation des clés dans le guide du AWS Key Management Service développeur.

Gestion des identités et des accès pour Amazon Detective

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. IAMles administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources Detective. IAMest un Service AWS stylo que vous pouvez utiliser sans frais supplémentaires.

Table des matières

- Public ciblé
- Authentification avec des identités
- Gestion des accès à l'aide de politiques
- Comment Amazon Detective travaille avec IAM
- Exemples de politiques basées sur l'identité d'Amazon Detective
- AWS politiques gérées pour Amazon Detective

- Utilisation des rôles liés aux services pour Detective
- Résolution de problèmes pour Identité et accès Amazon Detective

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Detective.

Utilisateur du service : si vous utilisez le service Detective pour effectuer votre tâche, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Plus vous utiliserez de fonctionnalités Detective pour effectuer votre travail, plus vous aurez besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans Detective, consultez Résolution de problèmes pour Identité et accès Amazon Detective.

Administrateur du service : si vous êtes le responsable des ressources Detective de votre entreprise, vous bénéficiez probablement d'un accès total à Detective. Votre responsabilité est de déterminer les fonctionnalités Detective ainsi que les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette page pour comprendre les concepts de base deIAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM Detective, consultezComment Amazon Detective travaille avec IAM.

IAMadministrateur — Si vous êtes IAM administrateur, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Detective. Pour consulter des exemples de politiques basées sur l'identité Detective que vous pouvez utiliser dansIAM, consultez. Exemples de politiques basées sur l'identité d'Amazon Detective

Authentification avec 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 que Utilisateur racine d'un compte AWS, en tant qu'IAMutilisateur ou en assumant un IAM rôle.

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 (IAMIdentity 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 en tant qu'identité fédérée, votre administrateur a préalablement configuré la fédération d'identité à l'aide de IAM rôles. 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 version 4 de AWS Signature pour les API demandes dans le guide de IAM l'utilisateur.

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, voir Authentification multifactorielle dans le guide de l'AWS IAM Identity Center utilisateur et Authentification AWS multifactorielle IAM dans le guide de l'IAMutilisateur.

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 nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section Tâches nécessitant des informations d'identification utilisateur root dans le guide de IAM l'utilisateur.

Utilisateurs et groupes IAM

Un IAMutilisateur 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 IAM utilisateurs dotés d'informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme auprès des IAM utilisateurs, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, voir Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme dans le Guide de IAM l'utilisateur.

Un IAMgroupe est une identité qui définit un ensemble d'IAMutilisateurs. 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 nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

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 la section Cas d'utilisation pour IAM les utilisateurs dans le Guide de IAM l'utilisateur.

IAMRôles

Un IAMrôle est une identité au sein de Compte AWS vous dotée d'autorisations spécifiques. Il est similaire à un IAM utilisateur, mais n'est pas associé à une personne en particulier. Pour assumer temporairement un IAM rôle dans le AWS Management Console, vous pouvez passer d'un rôle d'utilisateur à un IAM rôle (console). Vous pouvez assumer un rôle en appelant une AWS API opération AWS CLI or ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section Méthodes pour assumer un rôle dans le Guide de IAM l'utilisateur.

IAMles rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- 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 plus d'informations sur les rôles pour la fédération, voir Créer un rôle pour un fournisseur d'identité tiers (fédération) dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un rôle

dans. IAM Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

- Autorisations IAM utilisateur temporaires : un IAM utilisateur ou un rôle peut assumer un IAM rôle afin d'obtenir temporairement différentes autorisations pour une tâche spécifique.
- Accès entre comptes : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à 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, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.
- 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 transmises (FAS) — Lorsque vous utilisez un IAM utilisateur ou un rôle 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. FASutilise les autorisations du principal appelant an Service AWS, combinées à la demande Service AWS pour adresser des demandes aux services en aval. FASles demandes 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 les politiques relatives FAS aux demandes, consultez la section Transférer les sessions d'accès.
  - Rôle de service — Un rôle de service est un IAMrôle qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, consultez la section Créer un rôle pour déléguer des autorisations à un Service AWS dans le guide de IAM l'utilisateur.
  - 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 IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui font AWS CLI des AWS API demandes. Cela est préférable au stockage des clés d'accès

dans l'EC2instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour 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 exécutés sur l'EC2instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utiliser un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le Guide de IAM l'utilisateur.

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 JSON documents. Pour plus d'informations sur la structure et le contenu des documents de JSON politique, voir Présentation des JSON politiques dans le guide de IAM l'utilisateur.

Les administrateurs peuvent utiliser AWS JSON des politiques 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 autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

IAMles politiques définissent les autorisations pour une action, quelle que soit la méthode que vous utilisez pour effectuer l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur doté de cette politique peut obtenir des informations sur le rôle auprès du AWS Management Console AWS CLI, ou du AWS API.

politiques basées sur l'identité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité,

voir Définir des IAM autorisations personnalisées avec des politiques gérées par le client dans le Guide de l'IAMutilisateur.

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 savoir comment choisir entre une politique gérée ou une politique intégrée, voir Choisir entre les politiques gérées et les politiques intégrées dans le Guide de l'IAMutilisateur.

Politiques basées sur une ressource

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. 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 de politiques AWS gérées depuis une IAM stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLssont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Amazon S3 et Amazon VPC sont des exemples de services compatiblesACLs. AWS WAF Pour en savoir plusACLs, consultez la présentation de la liste 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.

- Limites d'autorisations — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (IAMutilisateur ou rôle). 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 annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, voir Limites d'autorisations pour les IAM entités dans le Guide de IAM l'utilisateur.
- Politiques de contrôle des services (SCPs) : SCPs JSON politiques 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 des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Les SCP limites d'autorisations pour les entités présentes dans les comptes des membres, y compris chacune d'entre elles Utilisateur racine d'un compte AWS. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.
- Politiques de contrôle des ressources (RCPs) : RCPs JSON politiques que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les IAM politiques associées à chaque ressource que vous possédez. Cela RCP limite les autorisations pour les ressources dans les comptes des membres et peut avoir un impact sur les autorisations effectives pour les identités Utilisateur racine d'un compte AWS, y compris, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les OrganizationsRCPs, y compris une liste de ces Services AWS supportsRCPs, consultez la section Resource control policies (RCPs) dans le guide de AWS Organizations l'utilisateur.
- 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 la section Politiques de session dans le guide de IAM l'utilisateur.

Types de politique multiple

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 IAM l'utilisateur.

Comment Amazon Detective travaille avec IAM

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources Amazon Detective. Ils ne peuvent pas non plus effectuer de tâches à l'aide du AWS Management Console AWS CLI, ou AWS API. Un administrateur Detective doit disposer de politiques AWS Identity and Access Management (IAM) autorisant les IAM utilisateurs et les rôles à effectuer des API opérations spécifiques sur les ressources dont ils ont besoin. L'administrateur doit ensuite associer ces politiques au principal ayant besoin de ces autorisations.

Detective utilise des politiques IAM basées sur l'identité pour accorder des autorisations aux types d'utilisateurs et d'actions suivants :

- Comptes administrateurs : le compte administrateur est le propriétaire d'un graphe de comportement qui utilise les données de son compte. Les comptes administrateurs peuvent ensuite inviter d'autres comptes membres à apporter leurs données au graphe de comportement. Le compte administrateur peut également utiliser le graphe de comportement pour trier et étudier les résultats et les ressources associés à ces comptes.

  Vous pouvez configurer des politiques pour permettre à des utilisateurs autres que le compte administrateur d'effectuer différents types de tâches. Par exemple, un utilisateur d'un compte administrateur peut uniquement être autorisé à gérer les comptes membres. Un autre utilisateur peut uniquement être autorisé à utiliser le graphe de comportement à des fins d'enquête.
- Comptes membres : un compte membre est un compte qui est invité à fournir des données à un graphe de comportement. Un compte membre répond à une invitation. Après avoir accepté une invitation, un compte membre peut supprimer son compte du graphe de comportement.

Pour obtenir une vue d'ensemble de la façon dont Detective et d' Services AWS autres utilisent DetectiveIAM, consultez la section Création de politiques dans l'JSONonglet du guide de IAM l'utilisateur.

politiques basées sur l’identité Detective

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions et les ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Detective prend en charge des actions, ressources et clés de condition spécifiques.

Pour en savoir plus sur tous les éléments que vous utilisez dans une JSON politique, consultez la section Référence des éléments de IAM JSON stratégie dans le guide de IAM l'utilisateur.

Actions

Les administrateurs peuvent utiliser AWS JSON des politiques 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'`Action`élément d'une JSON politique décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès dans une politique. Les actions de stratégie portent généralement le même nom que l' AWS APIopération associée. Il existe certaines exceptions, telles que les actions avec autorisation uniquement qui n'ont pas d'opération correspondante. API Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d’actions dans une politique afin d’accorder l’autorisation d’exécuter les opérations associées.

Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. L’élément `Action` répertorie les actions autorisées par la politique. L’élément `NotAction` répertorie les actions qui ne sont pas autorisées.

Les actions définies pour Detective reflètent les tâches que vous pouvez effectuer à l’aide de Detective. Les actions stratégiques dans Detective ont le préfixe suivant :`detective:`.

Par exemple, pour autoriser l'utilisation de l'`CreateMembers`APIopération visant à inviter les comptes des membres à consulter un graphique de comportement, vous devez inclure l'`detective:CreateMembers`action dans leur politique.

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules. Par exemple, pour un compte membre, la politique inclut l'ensemble des actions liées à la gestion d'une invitation :

```
"Action": [
      "detective:ListInvitations",
      "detective:AcceptInvitation",
      "detective:RejectInvitation",
      "detective:DisassociateMembership
]
```

Vous pouvez utiliser des caractères génériques (*) pour spécifier plusieurs actions. Par exemple, pour gérer les données utilisées dans leur graphe de comportement, les comptes administrateurs de Detective doivent être en mesure d'effectuer les tâches suivantes :

- Consulter la liste de leurs comptes membres (`ListMembers`).
- Obtenir des informations sur les comptes membres sélectionnés (`GetMembers`).
- Inviter les comptes membres à accéder à leur graphe de comportement (`CreateMembers`).
- Supprimer les membres de leur graphe de comportement (`DeleteMembers`).

Au lieu de répertorier ces actions séparément, vous pouvez autoriser l'accès à toutes les actions qui se terminent par le mot `Members`. La politique à cet effet peut inclure les mesures suivantes :

```
"Action": "detective:*Members"
```

Pour afficher la liste des actions Detective, consultez Actions définies par Amazon Detective dans la Référence de l'autorisation de service.

Ressources

Les administrateurs peuvent utiliser AWS JSON des politiques 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 `Resource` JSON de stratégie indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de spécifier une ressource en utilisant son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions

qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour plus d'informations sur le format deARNs, consultez Amazon Resource Names (ARNs) et AWS Service Namespaces.

Pour Detective, le seul type de ressource est le graphe de comportement. La ressource de graphe comportemental de Detective contient les éléments suivants ARN :

```
arn:aws:detective:${Region}:${AccountId}:graph:${GraphId}
```

Par exemple, un graphe de comportement présente les valeurs suivantes :

- La région du graphe de comportement est `us-east-1`.
- L'ID de compte pour l'ID de compte administrateur est `111122223333`.
- L'ID du graphe de comportement est `027c7c4610ea4aacaf0b883093cab899`.

Pour identifier ce graphique de comportement dans une `Resource` instruction, vous devez utiliser ce qui suit ARN :

```
"Resource": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
```

Pour spécifier plusieurs ressources dans une instruction `Resource`, séparez-les par des virgules.

```
"Resource": [
      "resource1",
      "resource2"
]
```

Par exemple, le même AWS compte peut être invité à devenir membre dans plusieurs graphes de comportement. Dans la politique de ce compte membre, la déclaration `Resource` liste les graphes de comportement auxquels ils étaient invités.

```
"Resource": [
      "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
      "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
]
```

Certaines actions Detective, telles que la création d'un graphe de comportement, la liste des graphes de comportement et la liste des invitations à des graphes de comportement, ne sont pas effectuées sur un graphe de comportement spécifique. Pour ces actions, l'instruction `Resource` doit utiliser le caractère générique (*).

```
"Resource": "*"
```

Pour les actions du compte administrateur, Detective vérifie toujours que l'utilisateur à l'origine de la demande appartient au compte administrateur pour le graphe de comportement concerné. Pour les actions relatives au compte membre, Detective vérifie toujours que l'utilisateur qui fait la demande appartient au compte membre. Même si une IAM politique autorise l'accès à un graphe de comportement, si l'utilisateur n'appartient pas au bon compte, il ne peut pas effectuer l'action.

Pour toutes les actions effectuées sur un graphe de comportement spécifique, la IAM politique doit inclure le graphiqueARN. Le graphique ARN peut être ajouté ultérieurement. Par exemple, lorsqu'un compte active Detective pour la première fois, la IAM politique initiale permet d'accéder à toutes les actions de Detective, en utilisant le caractère générique du graphiqueARN. Cela permet à l'utilisateur de commencer immédiatement à gérer les comptes membres et à mener des enquêtes dans leur graphe de comportement. Une fois le graphe de comportement créé, vous pouvez mettre à jour la politique pour ajouter le graphiqueARN.

Clés de condition

Les administrateurs peuvent utiliser AWS JSON des politiques 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 autoriser un IAM utilisateur à accéder à une ressource uniquement si celle-ci est étiquetée avec son nom IAM d'utilisateur. Pour plus d'informations, consultez IAMla section Éléments de politique : variables et balises dans le Guide de IAM l'utilisateur.

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 contextuelles de condition AWS globales dans le guide de IAM l'utilisateur.

Detective ne définit pas son propre ensemble de clés de condition. Detective prend en charge l'utilisation de certaines clés de condition globales. Pour voir toutes les clés de condition AWS globales, voir Clés contextuelles de condition AWS globale dans le guide de IAM l'utilisateur.

Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon Detective.

Exemples

Pour voir des exemples de politiques Detective basées sur l'identité, consultez Exemples de politiques basées sur l'identité d'Amazon Detective.

Politiques basées sur les ressources Detective (non prises en charge)

Detective ne prend pas en charge les politiques basées sur les ressources.

Autorisation basée sur les balises du graphe de comportement Detective

Des valeurs de balise peuvent être attribuées à chaque graphe de comportement. Vous pouvez utiliser ces valeurs de balise dans les instructions de condition pour gérer l'accès au graphe de comportement.

L'instruction de condition pour une valeur de balise utilise le format suivant.

```
{"StringEquals"{"aws:ResourceTag/<tagName>": "<tagValue>"}}
```

Par exemple, utilisez le code suivant pour autoriser ou refuser une action lorsque la valeur de la balise `Department` est `Finance`.

```
{"StringEquals"{"aws:ResourceTag/Department": "Finance"}}
```

Pour des exemples de politiques qui utilisent des valeurs de balise de ressource, consultez the section called "Compte administrateur : restriction de l'accès en fonction des valeurs de balise".

IAMRôles de Detective

Un IAMrôle est une entité de votre AWS compte qui possède des autorisations spécifiques.

Utilisation des informations d'identification temporaires avec Detective

Vous pouvez utiliser des informations d'identification temporaires pour vous connecter à la fédération, assumer un IAM rôle ou assumer un rôle entre comptes. Vous obtenez des informations d'identification de sécurité temporaires en appelant AWS STS API des opérations telles que AssumeRoleou GetFederationToken.

Detective prend en charge l'utilisation des informations d'identification temporaires.

Rôles liés à un service

Les rôles liés aux AWS services permettent aux services d'accéder aux ressources d'autres services pour effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre IAM compte et appartiennent au service. Un IAM administrateur peut consulter mais pas modifier les autorisations pour les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez the section called "Utilisation des rôles liés à un service".

Rôles de service (non pris en charge)

Cette fonctionnalité permet à un service d'endosser un rôle de service en votre nom. Ce rôle autorise le service à accéder à des ressources d'autres services pour effectuer une action en votre nom. Les rôles de service apparaissent dans votre IAM compte et sont détenus par le compte. Cela signifie qu'un IAM administrateur peut modifier les autorisations associées à ce rôle. Toutefois, une telle action peut perturber le bon fonctionnement du service.

Detective ne prend pas en charge les rôles de service.

Exemples de politiques basées sur l'identité d'Amazon Detective

Par défaut, IAM les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources Detective. Ils ne peuvent pas non plus effectuer de tâches à l'aide du AWS Management Console AWS CLI, ou AWS API.

Un IAM administrateur doit créer des IAM politiques qui accordent aux utilisateurs et aux rôles l'autorisation d'effectuer des API opérations spécifiques sur les ressources spécifiques dont ils ont besoin. L'administrateur associe ensuite ces politiques aux IAM utilisateurs ou aux groupes qui ont besoin de ces autorisations.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, voir Création de politiques dans l'JSONonglet du guide de l'IAMutilisateur.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Detective
- Autoriser des utilisateurs à afficher leurs propres autorisations
- Compte administrateur : gestion des comptes membres dans un graphe de comportement
- Compte administrateur : utilisation d'un graphe de comportement à des fins d'enquête
- Compte membre : gestion des invitations et des adhésions basées sur des graphes de comportement
- Compte administrateur : restriction de l'accès en fonction des valeurs de balise

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources Detective dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation

courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez les politiques AWS gérées ou les politiques AWS gérées pour les fonctions professionnelles dans le Guide de IAM l'utilisateur.

- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à IAM l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une 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 IAM pour appliquer des autorisations, consultez la section Politiques et autorisations du Guide de IAM l'utilisateur. IAM
- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez rédiger une condition de politique pour spécifier que toutes les demandes doivent être envoyées en utilisantSSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, voir Éléments IAM JSON de politique : Condition dans le guide de IAM l'utilisateur.
- Utilisez IAM Access Analyzer pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles. IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles respectent le langage des politiques (JSON) et IAM les IAM meilleures pratiques. IAMAccess Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez la section Valider les politiques avec IAM Access Analyzer dans le guide de l'IAMutilisateur.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des IAM utilisateurs ou un utilisateur root Compte AWS, activez-le MFA pour une sécurité supplémentaire. Pour exiger le MFA moment où les API opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez la section APIAccès sécurisé avec MFA dans le guide de IAM l'utilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de sécuritéIAM, consultez la section Bonnes pratiques en matière de sécurité IAM dans le Guide de IAM l'utilisateur.

Utilisation de la console Detective

Pour utiliser la console Amazon Detective, l'utilisateur ou le rôle doit avoir accès aux actions pertinentes, qui correspondent aux actions correspondantes dans leAPI.

Pour activer Detective et devenir un compte administrateur pour un graphe de comportement, l'utilisateur ou le rôle doit être autorisé à effectuer l'action `CreateGraph`.

Pour utiliser la console Detective afin d'effectuer des actions sur le compte administrateur, l'utilisateur ou le rôle doit être autorisé à effectuer cette action `ListGraphs`. Cela donne l'autorisation de récupérer les graphes de comportement dont le compte est un compte administrateur. Ils doivent également être autorisés à effectuer des actions spécifiques sur le compte administrateur.

Les actions les plus élémentaires du compte administrateur consistent à afficher la liste des comptes membres dans un graphe de comportement, et à utiliser le graphe de comportement à des fins d'enquête.

- Pour afficher la liste des comptes membres dans un graphe de comportement, le principal doit être autorisé à effectuer l'action `ListMembers`.
- Pour mener une enquête dans un graphe de comportement, le principal doit être autorisé à effectuer l'action `SearchGraph`.

Pour utiliser la console Detective afin d'effectuer des actions sur le compte membre, l'utilisateur ou le rôle doit être autorisé à effectuer cette action `ListInvitations`. Cela donne l'autorisation de consulter les invitations à des graphes de comportement. L'utilisateur ou le rôle peut ensuite être autorisé à effectuer des actions spécifiques sur le compte membre.

Autoriser des utilisateurs à afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux IAM utilisateurs de consulter les politiques intégrées et gérées associées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide du AWS CLI ou. AWS API

```
{
    "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": "*"
        }
    ]
}
```

Compte administrateur : gestion des comptes membres dans un graphe de comportement

Cet exemple de politique est destiné aux utilisateurs de comptes administrateurs qui sont uniquement responsables de la gestion des comptes membres utilisés dans le graphe de comportement. Cette politique permet également à l'utilisateur de consulter les informations d'utilisation et de désactiver Detective. Cette politique n'autorise pas l'utilisation du graphe de comportement à des fins d'enquête.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":
["detective:ListMembers","detective:CreateMembers","detective:DeleteMembers","detective:DeleteG
```

```
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
  },
  {
    "Effect":"Allow",
    "Action":["detective:CreateGraph","detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

Compte administrateur : utilisation d'un graphe de comportement à des fins d'enquête

Cet exemple de politique est destiné aux utilisateurs de comptes administrateurs qui utilisent le graphe de comportement uniquement à des fins d'enquête. Ils ne peuvent ni consulter ni modifier la liste des comptes membres dans le graphe de comportement.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":["detective:SearchGraph"],
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
   },
   {
    "Effect":"Allow",
    "Action":["detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

Compte membre : gestion des invitations et des adhésions basées sur des graphes de comportement

Cet exemple de politique est destiné aux utilisateurs appartenant à un compte membre. Dans l'exemple, le compte membre appartient à deux graphes de comportement. La politique accorde l'autorisation de répondre aux invitations et de supprimer le compte membre du graphe de comportement.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
   "Action":
["detective:AcceptInvitation","detective:RejectInvitation","detective:DisassociateMembership"],
   "Resource":[
       "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
       "arn:aws:detective:us-
east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
    ]
  },
  {
    "Effect":"Allow",
    "Action":["detective:ListInvitations"],
    "Resource":"*"
  }
 ]
}
```

Compte administrateur : restriction de l'accès en fonction des valeurs de balise

La politique suivante permet à l'utilisateur d'utiliser un graphe de comportement pour déterminer si la balise `SecurityDomain` du graphe de comportement correspond à la balise `SecurityDomain` de l'utilisateur.

```
{
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Allow",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals"{
                "aws:ResourceTag/SecurityDomain": "aws:PrincipalTag/SecurityDomain"
            }
        }
    },
    {
        "Effect":"Allow",
        "Action":["detective:ListGraphs"],
```

```
        "Resource":"*"
    } ]
}
```

La politique suivante empêche les utilisateurs d'utiliser un graphe de comportement pour étudier si la valeur de la balise `SecurityDomain` pour le graphe de comportement est `Finance`.

```
{
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Deny",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals": {"aws:ResourceTag/SecurityDomain": "Finance"}
        }
    } ]
}
```

AWS politiques gérées pour Amazon Detective

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AmazonDetectiveFullAccess

Vous pouvez associer la politique `AmazonDetectiveFullAccess` à vos identités IAM.

Cette politique accorde des autorisations administratives qui permettent à un principal d'accéder pleinement à toutes les actions Amazon Detective. Vous pouvez attacher cette politique à un principal avant qu'il n'active Detective pour son compte. Il doit également être associé au rôle utilisé pour exécuter les scripts Python Detective afin de créer et de gérer un graphe de comportement.

Les principaux disposant de ces autorisations peuvent gérer les comptes des membres, ajouter des balises à leur graphe de comportement et utiliser Detective pour leurs enquêtes. Ils peuvent également archiver GuardDuty les résultats. La politique fournit les autorisations dont la console Detective a besoin pour afficher les noms des comptes enregistrés AWS Organizations.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `detective` : donne aux principals un accès total à toutes les actions de Detective.
- `organizations` : permet aux principals d'accéder à des informations AWS Organizations sur les comptes d'une organisation. Si un compte appartient à une organisation, ces autorisations permettent à la console Detective d'afficher les noms des comptes en plus des numéros de compte.
- `guardduty`— Permet aux directeurs d'obtenir et d'archiver GuardDuty les résultats depuis Detective.
- `securityhub` : permet aux principal d'accéder aux résultats du Security Hub depuis Detective.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "detective:*",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ArchiveFindings"
            ],
            "Resource": "arn:aws:guardduty:*:*:detector/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:GetFindings",
                "guardduty:ListDetectors"

            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "securityHub:GetFindings"
            ],
            "Resource": "*"
         }
    ]
}
```

AWS politique gérée : AmazonDetectiveMemberAccess

Vous pouvez également associer la politique `AmazonDetectiveMemberAccess` à vos entités IAM.

Cette politique fournit aux membres un accès à Amazon Detective et un accès limité à la console.

Grâce à cette politique, vous pouvez :

- Consulter les invitations à devenir membre Detective par graphe, et accepter ou refuser ces invitations.
- Découvrir comment votre activité dans Detective contribue au coût d'utilisation de ce service sur la page Utilisation.
- Résilier votre adhésion dans un graphe.

Cette politique accorde des autorisations qui permettent d'accéder en lecture seule à la console Detective.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `detective` : permet aux membres d'accéder à Detective.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource": "*"
    }
  ]
}
```

Politique gérée par AWS : AmazonDetectiveInvestigatorAccess

Vous pouvez associer la politique `AmazonDetectiveInvestigatorAccess` à vos entités IAM.

Cette politique fournit aux enquêteurs un accès au service Detective et un accès limité aux dépendances de l'interface utilisateur de la console Detective. Cette politique accorde des autorisations permettant d'activer les enquêtes Detective dans Detective pour les rôles et utilisateurs

IAM. Vous pouvez mener une enquête pour identifier les indicateurs de compromission, tels que les résultats, à l'aide d'un rapport d'enquête, qui fournit des analyses et des informations sur les indicateurs de sécurité. Le rapport est classé par gravité, qui est déterminée à l'aide de l'analyse comportementale et du machine learning de Detective. Vous pouvez utiliser le rapport pour prioriser la correction des ressources.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `detective` : permet aux enquêteurs principals d'accéder aux actions de Detective, d'effectuer des enquêtes Detective, et d'élaborer un résumé des groupes de résultats.
- `guardduty`— Permet aux directeurs d'obtenir et d'archiver GuardDuty les résultats depuis Detective.
- `securityhub` : permet aux principal d'accéder aux résultats du Security Hub depuis Detective.
- `organizations`— Permet aux directeurs de récupérer des informations sur les comptes d'une organisation auprès de AWS Organizations. Si un compte appartient à une organisation, ces autorisations permettent à la console Detective d'afficher les noms des comptes en plus des numéros de compte.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DetectivePermissions",
      "Effect": "Allow",
      "Action": [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
```

```
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
        "detective:ListIndicators",
        "detective:InvokeAssistant"
      ],
      "Resource": "*"
    },
    {
      "Sid": "OrganizationsPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GuardDutyPermissions",
      "Effect": "Allow",
      "Action": [
        "guardduty:ArchiveFindings",
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SecurityHubPermissions",
      "Effect": "Allow",
      "Action": [
        "securityHub:GetFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS politique gérée : AmazonDetectiveOrganizationsAccess

Vous pouvez associer la politique `AmazonDetectiveOrganizationsAccess` à vos entités IAM.

Cette politique autorise l'activation et la gestion d'Amazon Detective au sein d'une organisation. Vous pouvez activer Detective dans l'ensemble de l'organisation et déterminer le compte administrateur délégué pour Detective.

Détails des autorisations

Cette politique inclut les autorisations suivantes :

- `detective` : permet aux principals d'accéder aux actions de Detective.
- `iam` : spécifie qu'un rôle lié à un service est créé lorsque Detective appelle `EnableOrganizationAdminAccount`.
- `organizations`— Permet aux directeurs de récupérer des informations sur les comptes d'une organisation auprès de AWS Organizations. Si un compte appartient à une organisation, ces autorisations permettent à la console Detective d'afficher les noms des comptes en plus des numéros de compte. Permet l'intégration d'un AWS service, permet d'enregistrer et de désenregistrer le compte de membre spécifié en tant qu'administrateur délégué, et permet aux principaux de récupérer les comptes d'administrateur délégué dans d'autres services de sécurité tels qu'Amazon Detective, Amazon, Amazon GuardDuty Macie et. AWS Security Hub

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource": "*"
    },
    {
```

```
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
```

```
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com",
            "guardduty.amazonaws.com",
            "macie.amazonaws.com",
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Politique gérée par AWS : AmazonDetectiveServiceLinkedRole

Vous ne pouvez pas associer `AmazonDetectiveServiceLinkedRole` à vos entités IAM. Cette politique est associée à un rôle lié au service qui permet à Detective d'effectuer des actions en votre nom. Pour plus d'informations, consultez the section called "Utilisation des rôles liés à un service".

Cette politique accorde des autorisations administratives qui permettent au rôle lié au service de récupérer des informations de compte pour une organisation.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `organizations` : récupère les informations de compte d'une organisation.

```
{
  "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "organizations:DescribeAccount",
              "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

Mises à jour détectives des politiques AWS gérées

Consultez les détails des mises à jour apportées aux politiques AWS gérées pour Detective depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la Page historique du document .

Modification	Description	Date
AmazonDetectiveInvestigatorAccess : mise à jour des politiques existantes	Des récapitulatifs de groupes de résultats et d'enquêtes Detective ont été ajoutés à la politique `AmazonDetectiveInvestigatorAccess` . Ces actions permettent de démarrer, de récupérer et de mettre à jour les enquêtes de Detective, ainsi que d'obtenir un résumé des groupes de résultats trouvés dans Detective.	26 novembre 2023
AmazonDetectiveFullAccess et AmazonDetectiveInvestigatorAccess : mises à jour des politiques existantes	Actions `GetFindings` Security Hub ajoutées par Detective aux politiques `AmazonDetectiveFullAccess` et `AmazonDetectiveInvestigatorAccess` . Ces actions permettent d'obtenir les résultats de Security Hub depuis Detective.	16 mai 2023
AmazonDetectiveOrganizationsAccess : nouvelle politique	Politique `AmazonDetectiveOrganizationsAccess` ajoutée par Detective.	02 mars 2023

Modification	Description	Date
	Cette politique autorise l'activation et la gestion de Detective au sein d'une organisation	
AmazonDetectiveMemberAccess : nouvelle politique	Politique `AmazonDetectiveMemberAccess` ajoutée par Detective. Cette politique fournit aux membres un accès à Detective et un accès limité aux dépendances de l'interface utilisateur de la console.	17 janvier 2023
AmazonDetectiveFullAccess : mises à jour d'une politique existante	Detective a ajouté des GuardDuty `GetFindings` actions à la `AmazonDetectiveFullAccess` politique. Ces actions permettent d'obtenir GuardDuty des résultats depuis Detective.	17 janvier 2023
AmazonDetectiveInvestigatorAccess : nouvelle politique	Politique `AmazonDetectiveInvestigatorAccess` ajoutée par Detective. Cette politique permet au principal de mener des enquêtes dans Detective.	17 janvier 2023

Modification	Description	Date
AmazonDetectiveServiceLinkedRole : nouvelle politique	Detective a ajouté une nouvelle politique pour son rôle lié à un service. La politique permet au rôle lié à un service de récupérer des informations sur les comptes d'une organisation.	16 décembre 2021
Detective a commencé à suivre les changements	Detective a commencé à suivre les modifications apportées AWS à ses politiques gérées.	10 mai 2021

Utilisation des rôles liés aux services pour Detective

Amazon Detective utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM lié directement à Detective. Les rôles liés au service sont prédéfinis par Detective et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service simplifie la configuration de Detective car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. Detective définit les autorisations de ses rôles liés à un service ; sauf définition contraire, seul Detective peut endosser ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Vos ressources Detective sont ainsi protégées, car vous ne pouvez pas involontairement supprimer l'autorisation d'accéder aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM et recherchez les services qui comportent Oui dans la colonne Rôle lié à un service. Sélectionnez un Yes (Oui) avec un lien permettant de consulter la documentation du rôle lié à un service, pour ce service.

Autorisations des rôles liés à un service pour Detective

Detective utilise le rôle lié au service nommé AWSServiceRoleForDetective— Autorise le détective à accéder aux AWS Organizations informations en votre nom.

Le rôle AWSServiceRoleForDetective lié à un service fait confiance aux services suivants pour assumer le rôle :

- `detective.amazonaws.com`

Le rôle AWSServiceRoleForDetective lié à un service utilise la politique gérée. `AmazonDetectiveServiceLinkedRolePolicy`

Pour en savoir plus sur les mises à jour de la `AmazonDetectiveServiceLinkedRolePolicy` politique, consultez les mises à jour des politiques AWS gérées par Amazon Detective. Pour recevoir des alertes automatiques concernant les modifications apportées à cette politique, abonnez-vous au flux RSS sur la page d'historique des documents Detective.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour Detective

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous désignez le compte d'administrateur Detective pour une organisation dans l'API AWS Management Console AWS CLI, le ou l' AWS API, Detective crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous désignez le compte administrateur Detective d'une organisation, Detective crée à nouveau automatiquement le rôle lié au service.

Modification d'un rôle lié à un service pour Detective

Detective ne vous autorise pas à modifier le rôle AWSServiceRoleForDetective lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour Detective

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le service Detective utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression peut échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources Detective utilisées par AWSServiceRoleForDetective

1. Suppression du compte administrateur Detective. veuillez consulter the section called "Désignation du compte administrateur Detective".
2. Répétez le processus dans chaque région où vous avez désigné le compte administrateur Detective.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForDetective service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service Detective

Detective prend en charge l'utilisation des rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Régions et Points de terminaison AWS.

Résolution de problèmes pour Identité et accès Amazon Detective

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Detective andIAM. Si vous rencontrez des problèmes de refus d'accès ou des difficultés similaires lorsque vous travaillez avec AWS Identity and Access Management(IAM), consultez les IAM rubriques de résolution des problèmes du guide de IAM l'utilisateur.

Je ne suis pas autorisé à effectuer une action dans Detective

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe.

L'exemple d'erreur suivant se produit lorsque l'`mateojackson`IAMutilisateur essaie d'utiliser la console pour accepter une invitation à devenir membre d'un graphe de comportement, mais qu'il ne dispose pas des `detective:AcceptInvitation` autorisations nécessaires.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: detective:AcceptInvitation on resource: arn:aws:detective:us-
east-1:444455556666:graph:567856785678
```

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource `arn:aws:detective:us-east-1:444455556666:graph:567856785678` à l'aide de l'action `detective:AcceptInvitation`.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter l'action `iam:PassRole`, vos politiques doivent être mises à jour afin de vous permettre de transmettre un rôle à Detective.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un IAM utilisateur nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Detective. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes ressources Detective

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 (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Detective prend en charge ces fonctionnalités, consultez Comment Amazon Detective travaille avec IAM.
- Pour savoir comment donner accès à vos ressources sur un site Comptes AWS qui vous appartient, consultez la section Fournir l'accès à un IAM utilisateur dans un autre site Compte AWS que vous possédez dans le Guide de IAM l'utilisateur.
- 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 IAM l'utilisateur.
- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section Fournir un accès aux utilisateurs authentifiés de manière externe (fédération d'identité) dans le guide de l'IAMutilisateur.
- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, voir Accès aux ressources entre comptes IAM dans le guide de l'IAMutilisateur.

Validation de la conformité pour Amazon Detective

Amazon Detective est concerné par le programme AWS d'assurance. Pour plus d'informations, voir Health Information Trust Alliance Common Security Framework (HITRUST) CSF .

Pour une liste des AWS services concernés par des programmes de conformité spécifiques, voir AWSServices concernés par programme de conformité AWS . 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 .

AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité Guides sur la sécurité et la conformité — Les guides de sécurité et de conformité abordent les considérations architecturales et fournissent des étapes pour déployer des environnements de base axés sur la sécurité et la conformité sur lesquels AWS.
- Évaluation des ressources à l'aide des règles énoncées dans le 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— Ce AWS service fournit une vue complète de l'état de votre sécurité interne, AWS ce qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.

Résilience dans Amazon Detective

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Outre l'infrastructure AWS mondiale, Detective utilise la résilience intégrée à Amazon DynamoDB et Amazon Simple Storage Service (Amazon S3). Pour plus d'informations, consultez Résilience et reprise après sinistre dans Amazon DynamoDB et Résilience dans Amazon Simple Storage Service.

L'architecture Detective résiste également à la défaillance d'une seule zone de disponibilité. Cette résilience est intégrée à Detective et ne nécessite aucune configuration.

Sécurité de l'infrastructure dans Amazon Detective

En tant que service géré, Amazon Detective ; est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez les API appels AWS publiés pour accéder à Detective ; via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Sécurité de la couche de transport (TLS). Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Des suites de chiffrement parfaitement confidentielles (PFS) telles que (Ephemeral Diffie-Hellman) ou DHE 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 identifiant de clé d'accès et d'une clé d'accès secrète associés à un IAM principal. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Bonnes pratiques en matière de sécurité pour Detective

Detective fournit différentes fonctionnalités de sécurité à prendre en compte lorsque vous développez et implémentez vos propres politiques de sécurité. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

Pour Detective, les meilleures pratiques en matière de sécurité sont associées à la gestion des comptes dans un graphe de comportement.

Bonnes pratiques pour les comptes d'administrateur de Detective

Lorsque vous invitez des comptes membres sur votre graphique de comportement de Detective, invitez uniquement les comptes que vous supervisez.

Limitez l’accès au graphe de comportement. Les utilisateurs dotés de cette AmazonDetectiveFullAccesspolitique peuvent autoriser l'accès à toutes les actions de Detective. Les principaux disposant de ces autorisations peuvent gérer les comptes des membres, ajouter des balises à leur graphe de comportement et utiliser Detective pour leurs enquêtes. Lorsqu’un utilisateur a accès à un graphe de comportement, il peut voir tous les résultats relatifs aux comptes des membres. De tels résultats peuvent révéler des informations de sécurité sensibles.

Bonnes pratiques relatives aux comptes membres

Lorsque vous recevez une invitation à consulter un graphe de comportement, assurez-vous de valider la source de l’invitation.

Vérifiez l'identifiant du AWS compte administrateur qui a envoyé l'invitation. Vérifiez que vous savez à qui appartient le compte, et que le compte invitant a une raison légitime de surveiller vos données de sécurité.

Enregistrement des API appels Amazon Detective avec AWS CloudTrail

Detective est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Detective. CloudTrail capture tous les API appels à Detective sous forme d'événements. Les appels capturés incluent des appels provenant de la console Detective et des appels de code destinés aux API opérations de Detective.

- Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Detective.
- Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements.

À l'aide des informations collectées par CloudTrail, vous pouvez déterminer ce qui suit :

- La demande qui a été adressée à Detective
- L'adresse IP à partir de laquelle la demande a été effectuée
- La personne ayant effectué la demande
- Le moment où la demande a été formulée
- Des détails supplémentaires sur la demande

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations de détective dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans Detective, cette activité est enregistrée dans un CloudTrail événement, ainsi que d'autres événements de AWS service, dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS . Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris ceux de Detective, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3.

Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions AWS . Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. Vous pouvez également configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence.

Pour plus d'informations, consultez les ressources suivantes :

- Vue d'ensemble de la création d'un journal d'activité
- CloudTrail Services et intégrations pris en charge
- Configuration des SNS notifications Amazon pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

CloudTrail enregistre toutes les opérations de Detective, qui sont documentées dans le Detective API Reference.

Par exemple, les appels aux `DeleteMembers` opérations `CreateMembersAcceptInvitation`, et 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 faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM)
- Si la requête a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré
- Si la demande a été faite par un autre AWS service

Pour plus d'informations, consultez l'CloudTrail userIdentityélément.

Vue d'ensemble des entrées du fichier journal de Detective

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal.

Un événement représente une demande individuelle d'une source quelconque. Les événements incluent des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des API appels publics, de sorte que les entrées n'apparaissent pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`AcceptInvitation`action.


```
      {
            "EventId": "f2545ee3-170f-4340-8af4-a983c669ce37",
            "Username": "JaneRoe",
            "EventTime": 1571956406.0,
            "CloudTrailEvent": "{\"eventVersion\":\"1.05\",\"userIdentity\":
{\"type\":\"AssumedRole\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS:JaneRoe\",\"arn
\":\"arn:aws:sts::111122223333:assumed-role/1A4R5SKSPGG9V/JaneRoe\",\"accountId
\":\"111122223333\",\"accessKeyId\":\"AKIAIOSFODNN7EXAMPLE\",\"sessionContext\":
{\"attributes\":{\"mfaAuthenticated\":\"false\",\"creationDate\":\"2019-10-24T21:54:56Z
\"},\"sessionIssuer\":{\"type\":\"Role\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS
\",\"arn\":\"arn:aws:iam::111122223333:role/1A4R5SKSPGG9V\",\"accountId\":
\"111122223333\",\"userName\":\"JaneRoe\"}}},\"eventTime\":\"2019-10-24T22:33:26Z
\",\"eventSource\":\"detective.amazonaws.com\",\"eventName\":\"AcceptInvitation
\",\"awsRegion\":\"us-east-2\",\"sourceIPAddress\":\"192.0.2.123\",\"userAgent
\":\"aws /3 aws-sdk-java/1.11.648 Linux/4.14.133-97.112.amzn2.x86_64 OpenJDK_64-
Bit_Server_VM/25.201-b09 java/1.8.0_201 vendor/Oracle_Corporation exec-env/
AWS_Lambda_java8\",\"errorCode\":\"ValidationException\",\"requestParameters\":
{\"masterAccount\":\"111111111111\"},\"responseElements\":{\"message\":\"Invalid
 request body\"},\"requestID\":\"8437ff99-5ec4-4b1a-8353-173be984301f\",\"eventID\":
\"f2545ee3-170f-4340-8af4-a983c669ce37\",\"readOnly\":false,\"eventType\":\"AwsApiCall
\",\"recipientAccountId\":\"111122223333\"}",
            "EventName": "AcceptInvitation",
            "EventSource": "detective.amazonaws.com",
            "Resources": []
        },
```

Régions et quotas Amazon Detective

Lorsque vous utilisez Amazon Detective, soyez conscient de ces quotas.

Régions et points de terminaison de Detective

Pour voir la liste des Régions AWS endroits où Detective est disponible, consultez la section Points de terminaison du service Detective.

Quotas de Detective

Detective possède les quotas suivants, qui ne peuvent pas être configurés.

Ressource	Quota	Commentaires
Nombre de comptes membres	1 200	Nombre de comptes membres qu'un compte administrateur peut ajouter à un graphe de comportement.
Volume de données du graphe de comportement : avertissement de volume	9 To par jour	Si le volume de données du graphe de comportement est supérieur à 9 To par jour, Detective affiche un avertissement indiquant que le graphe de comportement est proche du volume maximal autorisé.
Volume de données du graphe de comportement : aucun nouveau compte	10 To par jour	Si le volume de données du graphe de comportement est supérieur à 10 To par jour, vous ne pouvez pas ajouter de nouveaux comptes de membre au graphe de comportement.
Volume de données du graphe de comportement : arrête l'ingestion de données dans le graphe de comportement	15 To par jour	Si le volume de données du graphe de comportement est supérieur à 15 To par jour, Detective arrête l'ingestion des données dans le graphe de comportement.

Ressource	Quota	Commentaires
		Les 15 To par jour reflètent à la fois le volume de données normal et les pics de volume de données. Pour réactiver l'ingestion de données, vous devez contacter Support.

Internet Explorer 11 n'est pas pris en charge

Vous ne pouvez pas utiliser Detective avec Internet Explorer 11.

Gestion des balises pour un graphe de comportement

Une étiquette est une étiquette facultative que vous pouvez définir et attribuer à AWS des ressources, notamment à certains types de ressources Detective. 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. 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 à votre graphe de comportement. Vous pouvez ensuite utiliser les valeurs des balises dans les IAM politiques pour gérer l'accès aux fonctions du graphe comportemental dans Detective. Consultez the section called “Autorisation basée sur les balises du graphe de comportement Detective”.

Vous pouvez également utiliser les balises comme outil de rapport des coûts. Par exemple, pour suivre les coûts associés à la sécurité, vous pouvez attribuer le même tag à votre graphe de comportement Detective, à la ressource du AWS Security Hub hub et aux GuardDuty détecteurs Amazon. Dans AWS Cost Explorer, vous pouvez ensuite rechercher cette balise pour obtenir une vue consolidée des coûts liés à ces ressources.

Afficher les balises d'un graphe de comportement

Vous pouvez gérer les balises de votre graphe de comportement à partir de la page Général.

Console

Pour afficher la liste des balises attribuées au graphe de comportement

1. Ouvrez la console Amazon Detective à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation, sous Paramètres, choisissez Général.

Detective API, AWS CLI

Vous pouvez utiliser le Detective API ou le AWS Command Line Interface pour obtenir la liste des balises de votre graphe de comportement.

Pour obtenir la liste des balises d'un graphe de comportement (DetectiveAPI, AWS CLI)

- Detective API : Utilisez l'`ListTagsForResource`opération. Vous devez fournir le graphique ARN de votre comportement.
- AWS CLI: À l'invite de commande, exécutez la commande `list-tags-for-resource`.

```
aws detective list-tags-for-resource --resource-arn <behavior graph ARN>
```

Exemple

```
aws detective list-tags-for-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Ajouter des balises à un graphe de comportement

Console

Dans la liste des balises de la page Général, vous pouvez ajouter des valeurs de balises au graphe de comportement.

Pour ajouter une balise à votre graphe de comportement

1. Sélectionnez Ajouter une nouvelle balise.
2. Pour Clé, entrez le nom de la balise.
3. Pour Valeur, saisissez la valeur de l'identification.

Detective API, AWS CLI

Vous pouvez utiliser le Detective API ou le AWS CLI pour ajouter des valeurs de balise à votre graphe de comportement.

Pour ajouter des balises à un graphe de comportement (DetectiveAPI, AWS CLI)

- Detective API : Utilisez l'`TagResource`opération. Vous fournissez le graphe de comportement ARN et les valeurs de balise à ajouter.
- AWS CLI : À l'invite de commande, exécutez la commande `tag-resource`.

```
aws-detective tag-resource --aws detective tag-resource --resource-arn <behavior
 graph ARN> --tags '{"TagName":"TagValue"}'
```

Exemple

```
aws detective tag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tags '{"Department":"Finance"}'
```

Supprimer des balises d'un graphe de comportement

Console

Pour supprimer un tag de la liste de la page Général, choisissez l'option Supprimer pour ce tag.

Detective API, AWS CLI

Vous pouvez utiliser le Detective API ou le AWS CLI pour supprimer les valeurs des balises de votre graphe de comportement.

Pour supprimer des balises d'un graphe de comportement (DetectiveAPI, AWS CLI)

- Detective API : Utilisez l'`UntagResource`opération. Vous fournissez le graphe ARN de comportement et les noms des balises à supprimer.
- AWS CLI : À l'invite de commande, exécutez la commande `untag-resource`.

```
aws detective untag-resource --resource-arn <behavior graph ARN> --tag-keys
 "TagName"
```

Exemple

```
aws detective untag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tag-keys "Department"
```

Désactivation Amazon Detective

Le compte administrateur d'un graphe de comportement peut désactiver Amazon Detective depuis la console Detective, l'API Detective ou AWS Command Line Interface. Lorsque vous désactivez Detective, le graphe de comportement et les données Detective associées sont supprimés.

Une fois qu'un graphe de comportement est supprimé, il ne peut pas être restauré.

Table des matières

- Désactiver Detective (console)
- Désactiver Detective (Detective API, AWS CLI)
- Désactiver Detective across Regions (script Python activé GitHub)

Désactiver Detective (console)

Vous pouvez désactiver Amazon Detective depuis la AWS Management Console.

Pour désactiver Amazon Detective (console)

1. Ouvrez la console Amazon à l'adresse https://console.aws.amazon.com/detective/.
2. Dans le volet de navigation Detective, sous Paramètres, choisissez Général.
3. Sur la page Général, sous Désactiver Amazon Detective, sélectionnez Désactiver Amazon Detective.
4. Lorsque vous êtes invité à confirmer, tapez **`disable`**.
5. Choisissez Désactiver Amazon Detective.

Désactiver Detective (Detective API, AWS CLI)

Vous pouvez désactiver Amazon Detective depuis l'API Detective ou l' AWS Command Line Interface. Pour obtenir l'ARN de votre graphe de comportement à utiliser dans la demande, utilisez l'opération `ListGraphs`.

Pour désactiver Detective (Detective API, AWS CLI)

- API Detective : utilisez l'opération `DeleteGraph`. Vous devez fournir l'ARN du graphe.

- AWS CLI: À l'invite de commande, exécutez la commande `delete-graph`.

```
aws detective delete-graph --graph-arn <graph ARN>
```

Exemple :

```
aws detective delete-graph --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Désactiver Detective across Regions (script Python activé GitHub)

Detective fournit un script open source GitHub qui vous permet de désactiver Detective pour un compte administrateur dans une liste spécifiée de régions.

Pour plus d'informations sur la configuration et l'utilisation GitHub des scripts, consultezthe section called "Scripts Python d'Amazon Detective".

Historique du document pour le guide de l’utilisateur Detective

Le tableau suivant décrit les modifications importantes apportées à la documentation depuis la dernière version de Detective. Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

- Dernière mise à jour de la documentation : 20 février 2025

Modification	Description	Date
Ajout de la prise en charge des résultats des séquences d' GuardDuty attaque Amazon	Detective a ajouté la prise en charge de la recherche des types associés à la détection GuardDuty étendue des menaces. GuardDutydétecte une séquence d'attaque lorsqu'une séquence spécifiqu e de plusieurs actions, telles que les activités d'API et la détection des GuardDuty résultats, correspond à une activité potentiellement suspecte. Pour plus d'informa tions sur la détection étendue des menaces et les types de détection de séquences d'attaques, consultez la section Extended Threat Detection dans le guide de GuardDuty l'utilisateur Amazon.	20 février 2025

Ajout de la prise en charge de la recherche d'Amazon GuardDuty IAM	Detective a ajouté la prise en charge d'un nouveau type de GuardDuty recherche qui vous alerte lorsque des informations d'identification utilisateur restreintes, créées pour les personnes répertoriées Comptes AWS dans votre environnement, sont utilisées pour envoyer des demandes à Services AWS. Pour de plus amples informations, consultez .Policy:IAMUser/ShortTermRootCredentialUsagedans le guide de GuardDuty l'utilisateur Amazon.	4 février 2025
Nouvelle fonction	Ajout d'une mise en page chronologique à Detective Finding Group Visualization. Ajout de la fonctionnalité du bouton de lecture et du filtrage des résultats basé sur la gravité. Ces améliorations peuvent vous aider à mieux comprendre la progression des événements, à hiérarchiser les problèmes critiques et à mener des enquêtes de sécurité plus efficaces.	27 décembre 2024

Ajout de la prise en charge des GuardDuty résultats d'Amazon	Detective a ajouté la prise en charge des trois GuardDuty types de détection suivants qui vous avertissent lorsque des commandes suspectes sont exécutées sur une EC2 instance Amazon ou une charge de travail de conteneur au sein de votre AWS environnement : • Discovery:Runtime/SuspiciousCommand • Persistence:Runtime/SuspiciousCommand • PrivilegeEscalation:Runtime/SuspiciousCommand	6 novembre 2024
Ajout de la prise en charge des GuardDuty résultats d'Amazon	Detective prend désormais en charge les types de recherche suivants liés à la surveillance du temps GuardDuty d'exécution. • `Execution:Runtime/SuspiciousShell` • `PriviliegeEscalation:Runtime/ElevationToRoot`	27 août 2024

Ajout de la prise en charge des GuardDuty résultats d'Amazon	Detective fournit désormais un support pour la protection contre les GuardDuty malwares pour S3. Cela vous permet d'analyser les objets récemment chargés dans les compartiments Amazon S3 afin de détecter d'éventuels malwares ou chargements suspects, et de prendre des mesures pour les isoler avant qu'ils ne soient ingérés dans les processus en aval.	9 juillet 2024
Fonctionnalités mises à jour	Detective a ajouté une nouvelle disposition radiale au panneau de visualisation des groupes de recherche, afin d'améliorer la visualisation et de faciliter l'interprétation des données.	26 juin 2024
Nouvelles versions des sources de Security Lake	Outre la version source 1 (OCSF 1.0.0-rc.2), Detective ingère désormais les données de la version source 2 (OCSF 1.1.0) pour les sources Security Lake prises en charge par Detective.	15 mai 2024
Nouvelle source de journal de Security Lake	Vous pouvez utiliser l'intégration Detective avec Security Lake pour collecter des journaux et des événements à partir des journaux d'audit Amazon EKS.	15 mai 2024

Mise à jour de la documentation	Le contenu de l'Amazon Detective Administration Guide est désormais consolidé dans le Amazon Detective User Guide. Le support standard d'Amazon Detective Administration Guide arrivera à expiration le 8 mai 2024.	15 avril 2024
Ajout de la prise en charge des GuardDuty résultats d'Amazon	Detective prend désormais en charge les types de recherche suivants liés à la surveillance du temps GuardDuty d'exécution. • `Execution:Runtime/MaliciousFileExecuted` • `Execution:Runtime/SuspiciousTool` • `DefenseEvasion:Runtime/PtraceAntiDebugging` • `Execution:Runtime/SuspiciousCommand` • `DefenseEvasion:Runtime/SuspiciousCommand`	5 avril 2024

Suppression de l'obligation GuardDuty d'adhésion à Amazon	Il n'est plus nécessaire d'être GuardDuty client pour activer Amazon Detective. L'obligation d'avoir GuardDuty activé Detective sur votre compte pendant 48 heures avant d'activer Detective a été supprimée.	2 février 2024
Ajout de la prise en charge des GuardDuty résultats d'Amazon	Detective étend la prise en charge des types de recherche de GuardDuty EC2 Runtime Monitoring à ECS et aux EC2 ressources.	30 janvier 2024
Fonctionnalités mises à jour	Vous pouvez désormais lancer une enquête Detective depuis la page Investigations pour une ressource spécifique que vous souhaitez étudier. Detective recommande des ressources en fonction de son activité dans les résultats et les groupes de résultats. Detective Investigations vous permet d'étudier les utilisateurs et les rôles IAM à l'aide d'indicateurs de compromission, qui peuvent vous aider à déterminer si une ressource est impliquée dans un incident de sécurité.	16 janvier 2024

Fonctionnalités mises à jour	Vous pouvez désormais effectuer une enquête Detective depuis la page Enquêtes d'une ressource recommandée. Detective recommande des ressource s en fonction de son activité dans les résultats et les groupes de résultats. Detective Investigations vous permet d'étudier les utilisate urs et les rôles IAM à l'aide d'indicateurs de compromis sion, qui peuvent vous aider à déterminer si une ressource est impliquée dans un incident de sécurité.	26 décembre 2023
Modifications apportées à la façon dont Detective lit le trafic de flux pour le partage VPCs	Si vous utilisez un Amazon VPC partagé, il est possible que vous constatiez des modifications dans le trafic surveillé par Detective. Nous vous recommandons de consulter les modifications apportées dans Détails de l'activité pour le volume global du flux VPC afin de comprendr e les éventuels effets sur votre couverture et de voir comment Detective calcule les coûts prévisionnels afin de comprendre l'impact sur vos coûts de service.	20 décembre 2023

Disponibilité par région	Les régions Europe (Stockholm), Europe (Paris) et Canada (Centre) ont été ajoutées à la liste des AWS régions dans lesquelles l'intégration de Detective à Security Lake est disponible.	8 décembre 2023
Nouvelle fonction	Enquêtes Detective vous permet d'enquêter sur les utilisateurs et les rôles IAM à l'aide d'indicateurs de compromission, qui peuvent vous aider à déterminer si une ressource est impliquée dans un incident de sécurité.	26 novembre 2023
Nouvelle fonction	Par défaut, Detective génère automatiquement des récapitulatifs de groupes de résultats pour rechercher des groupes de résultats optimisés par l'intelligence artificielle (IA générative). Le récapitulatif des groupes de résultats analyse rapidement les relations entre les résultats et les ressources affectées, puis résume les menaces potentielles en langage naturel.	26 novembre 2023

Nouvelle fonction	L'intégration de Detective avec Security Lake vous permet d'interroger et de récupérer les données brutes du journal stockées par Security Lake. Grâce à cette intégration, vous pouvez collecter des journaux et des événements à partir CloudTrail des événements de gestion et des journaux de flux Amazon Virtual Private Cloud (Amazon VPC).	26 novembre 2023
Ajout d'informations sur les politiques gérées au chapitre sécurité	Des récapitulatifs de groupes de résultats et d'enquête s Detective ont été ajoutés à la politique `AmazonDetectiveInvestigatorAccess` .	26 novembre 2023
Affichage d'une vue d'ensemble d'un résultat	Si un résultat est corrélé à une activité plus importante, Detective vous invite désormais à accéder à ce groupe de résultats.	18 septembre 2023
Points de terminaison et quotas Amazon Detective	Detective est désormais disponible dans la région Israël (Tel Aviv).	25 août 2023

Visualisation améliorée des groupes de résultats	La visualisation des groupes de résultats Detective inclut désormais des groupes de résultats avec des résultats regroupés, rendant ainsi plus efficace l'analyse des preuves, des entités et des résultats connexes.	08 août 2023
Amélioration des groupes de résultats	Les groupes de résultats incluent désormais les résultats de vulnérabilité d'Amazon Inspector.	13 juin 2023
Ajout de la prise en charge d'Amazon GuardDuty Lambda Protection	Detective fournit désormais un support pour GuardDuty Lambda Protection.	26 mai 2023
Ajout AWS de résultats de sécurité sous la forme d'un nouveau package de source de données facultatif.	Detective fournit désormais les résultats AWS de sécurité sous forme de package de source de données facultati f. Ce package de source de données facultatif permet à Detective d'ingérer des données depuis Security Hub et d'ajouter ces données à votre graphe de comportem ent.	16 mai 2023
Ajout de la prise en charge des types de recherche Amazon GuardDuty EKS Runtime Monitoring	Detective prend désormais en charge les types de recherche GuardDuty EKS Runtime Monitoring.	3 mai 2023

Ajout de la prise en charge des types de recherche Amazon GuardDuty RDS Protection	Detective prend désormais en charge les types de recherche de GuardDuty RDS Protection.	20 avril 2023
Ajout de la prise en charge de types de GuardDuty recherche Amazon supplémentaires	Detective propose désormais des profils pour les types de GuardDuty recherche supplémentaires suivants : `DefenseEvasion: EC2UnusualDNSResolver` `DefenseEvasion: EvasionEC2UnusualDoHActivity` `DefenseEvasion: DefenseEvasionEC2UnusualDoTActivity`	12 avril 2023
Ajouts de nouveaux volets de console dans la console Detective pour aider les utilisateurs à sélectionner la politique gérée par AWS adaptée à leur cas d'utilisation spécifique.	Detective propose des politiques gérées pour choisir en toute sécurité les autorisations dont vous avez besoin.	3 avril 2023
Affichage du trafic de flux VPC pour les clusters EKS	Ajout d'une nouvelle section pour le trafic de flux Amazon Virtual Private Cloud (Amazon VPC) avec des clusters Amazon Elastic Kubernetes Service (Amazon EKS).	2 mars 2023

Le groupe de résultats inclut désormais une représentation visuelle dynamique du graphe de comportement Detective	Le groupe de résultats Detective inclut désormais une représentation visuelle dynamique du graphe de comportement Detective afin de mettre en évidence la relation entre les entités et les résultats au sein du groupe de résultats.	28 février 2023
Exportation des données de la page Detective Récapitulatif et de la page des résultats de recherche. Les données sont exportées au format CSV (valeurs séparées par des virgules).	Detective offre désormais la possibilité d'exporter des données vers votre navigateur depuis la console Detective.	7 février 2023
Ajout du volume global de flux VPC pour les charges de travail EKS Amazon EKS	Detective ajoute désormais des récapitulatifs visuels et des analyses sur vos journaux de flux cloud privé virtuel (VPC) à partir de vos charges de travail Amazon Elastic Kubernetes Service Amazon EKS.	19 janvier 2023

Ajout d'informations sur les politiques gérées au chapitre sécurité	Detective soutient désormais les actions « GuardDuty get findings » dans le cadre de AmazonDetectiveFullAccess cette politique. Le chapitre sur la sécurité fournit désormais des détails sur les nouvelles politiques gérées suivantes pour Detective : AmazonDetectiveMemberAccess et AmazonDetectiveInvestigatorAccess.	17 janvier 2023
Ajout de conservation des données	Avec Detective, vous pouvez accéder à un an de données historiques sur les événements.	20 décembre 2022
Ajout de l'option permettant de régler la durée de validité sur la page de récapitulatif.	Detective offre désormais la possibilité d'ajuster la durée de validité et de visualiser l'activité sur une période de 24 heures au cours des 365 jours précédents.	5 octobre 2022
Recherche d'un résultat ou d'une entité	Detective propose désormais une recherche insensible à la casse.	3 octobre 2022
Ajout de la possibilité de définir l'horodatage de la durée de validité	Detective propose désormais un moyen de configurer la préférence de format d'horodatage de la durée de validité. Cette préférence sera appliquée à tous les horodatages dans Detective.	3 octobre 2022

Termes ajoutés relatifs aux groupes de résultats	Detective prend désormais en charge des groupes de résultats qui relient les résultats connexes sur un seul écran afin de vous aider à enquêter sur les activités malveillantes potentielles dans votre environnement. À partir d'un profil de groupe de résultats, vous pouvez passer à des profils d'entités, et à des vues d'ensemble des résultats relatives à ce groupe.	3 août 2022
Ajout de nouveaux profils associés aux journaux d'audit Amazon EKS	Detective fournit désormais des profils qui vous permettent d'étudier les activités suivantes associées aux entités liées aux conteneurs : clusters Amazon EKS, images de conteneurs, pods Kubernetes et sujets Kubernetes.	26 juillet 2022

Ajout d'une nouvelle source de données facultative	Detective prend désormais en charge les journaux d'audit EKS en tant que package de source de données facultatif. Un compte administrateur peut activer cette nouvelle source de données pour son graphe de comportement existant. Cette source de données sera activée par défaut pour les graphes créés après cette date. Les administrateurs peuvent désactiver manuellement cette source de données à tout moment.	26 juillet 2022
Nouveau rôle lié à un service et nouvelle politique gérée pour Detective	Detective a désormais un rôle lié à un service, `AWSServiceRoleForDetective` . Le rôle lié à un service est utilisé pour accéder aux données Organizations en votre nom. Le rôle utilise une nouvelle politique gérée par `AmazonDetectiveServiceLinkedRolePolicy` .	16 décembre 2021

Intégration ajoutée avec AWS Organizations	Detective est désormais intégré à Organizations. Le compte de gestion de l'organisation désigne un compte administrateur Detective pour l'organisation. Le compte administrateur Detective peut afficher tous les comptes de l'organisation et activer ces comptes en tant que comptes membres dans le graphe du comportement de l'organisation.	16 décembre 2021
Remplacement des profils de résultats par des vues d'ensemble des résultats	Les profils de résultats contenaient des visualisations analysant l'activité de la ressource concernée. La nouvelle vue d'ensemble des résultats contient les détails des résultats GuardDuty obtenus et une liste des entités impliquées. À partir de la vue d'ensemble des résultats, vous pouvez passer aux profils des entités associées.	20 septembre 2021

Suppression de la limite des types de GuardDuty recherche pris en charge	Detective n'est plus limité à un ensemble sélection né de types de GuardDuty recherche. Detective recueille automatiquement les détails des résultats pour tous les types de résultats, et donne accès aux profils des entités associées.	20 septembre 2021
Lien vers les détails des résultats dans le volet de profil des résultats associé	Sur un profil d'entité, lorsque vous choisissez un résultat dans la liste des résultats associée, les détails des résultats sont affichés dans le volet de droite. La durée de validité est définie sur la fenêtre temporelle de résultats .	20 septembre 2021
Ajout de compartiments S3 aux types d'entités disponibles dans Detective	Detective fournit désormais des profils pour les compartim ents S3. Les profils de compartiment S3 fournissent des détails sur les principal s qui ont interagi avec le compartiment S3 et les opérations d'API qu'ils ont effectuées sur le compartiment S3.	20 septembre 2021

Nouvelle option pour générer Detective URLs dans Splunk	Le projet Splunk Trumpet vous permet d'envoyer AWS du contenu à Splunk. Le projet vous permet désormais d'ajouter Detective URLs pour accéder aux profils des GuardDuty résultats.	8 septembre 2021
Remplacé AKIDs dans les détails d'activité pour les comptes et les rôles	Sur les profils de compte, les détails de l'activité pour le volume global d'appels d'API indiquent désormais les utilisateurs ou les rôles au lieu des identifiants de clé d'accès (AKIDs). Sur les profils de rôle, les détails de l'activité pour le volume global d'appels d'API indiquent désormais les sessions de rôle au lieu de AKIDs. Pour les activités qui ont eu lieu avant cette modification, l'appelant est répertorié comme ressource inconnue.	14 juillet 2021

Ajout du service d'appel aux informations sur les appels d'API	Sur la console Detective, les informations sur les appels d'API incluent désormais le service qui a émis l'appel. Ajout d'une colonne Service aux listes relatives au volume global des appels d'API, aux appels d'API récemment observés et aux appels d'API dont le volume a augmenté. En ce qui concerne les détails d'activité relatifs au volume global d'appels d'API et les géolocalisations récemment observées, les méthodes d'API sont regroupées sous les services qui les ont émises. Pour les activités survenues avant cette modification, les méthodes d'API sont regroupées sous Service inconnu.	14 juillet 2021
Nouvel onglet Interaction avec les ressources pour les utilisateurs, les rôles et les sessions de rôles	L'onglet Interaction avec les ressources pour les utilisateurs, les rôles et les sessions de rôles contient des informations sur les activités d'attribution de rôles impliquant ces entités. Pour les sessions de rôles, il s'agit d'un nouvel onglet. Pour les utilisateurs et les rôles, il s'agit d'un onglet existant avec du nouveau contenu.	29 juin 2021

Valeurs mises à jour pour les quotas de volume de données des graphes de comportement	Les quotas de volume de données pour les graphes de comportement ont été augmentés. À 3,24 To par jour, Detective émet un avertissement. À 3,6 To par jour, aucun nouveau compte ne peut être ajouté. À 4,5 To par jour, Detective arrête d'ingérer des données dans le graphe de comportement.	10 juin 2021
Valeurs de balise ajoutées aux options du script Python	Lorsque vous utilisez le script Python Detective `enableDetective.py` pour activer Detective, vous pouvez désormais attribuer des valeurs de balise au graphe de comportement.	19 mai 2021

Ajout de l'activation automatique des comptes membres qui réussissent le contrôle du volume de données	Lorsque les comptes membres acceptent une invitation, leur statut est Accepté (Non activé) jusqu'à ce que Detective vérifie que leurs données n'entraîneront pas un dépassement du quota par le volume de données du graphe de comportement. Si le volume de données ne pose aucun problème, Detective fait passer automatiquement le statut à Accepté (Activé). Notez que les comptes membres existants qui sont actuellement acceptés (non activés) ne peuvent pas être activés automatiquement.	12 mai 2021
Ajout d'informations sur les politiques gérées au chapitre sécurité	Une nouvelle section du chapitre sécurité fournit des détails sur les politiques gérées pour Detective. Detective fournit actuellement une politique gérée unique, `AmazonDetectiveFullAccess`.	10 mai 2021
Modification des valeurs du volume de données dans la liste des comptes membres	Sur la page de gestion des comptes, la liste des comptes membres affiche désormais le volume de données quotidien pour chaque compte membre. Auparavant, la liste affichait le volume en pourcentage du volume total autorisé.	29 avril 2021

Options révisées pour la gestion des comptes membres	Le menu Gérer les comptes a été remplacé par un menu Actions. Combinais on des options d'ajout de comptes individuels et d'ajout de comptes à partir d'un fichier .csv. L'option Activer les comptes a été déplacée de Gérer les comptes vers une option distincte située à côté de Actions.	5 avril 2021
Ajout de balises de graphe de comportement et d'une autorisation basée sur des balises	Lorsque vous activez Detective, vous pouvez ajouter des balises au graphe de comportement. Vous pouvez gérer les balises pour un graphe de comportement à partir de la page Général. Detective prend également en charge l'autorisation basée sur les valeurs des balises.	31 mars 2021

Ajout de la prise en charge de types de GuardDuty recherche Amazon supplémentaires	Detective propose désormais des profils pour les types de GuardDuty recherche supplémentaires suivants : `CredentialAccess:IAMUser/AnomalousBehavior` `DefenseEvasion:IAMUser/AnomalousBehavior` `Discovery:IAMUser/AnomalousBehavior` `Exfiltration:IAMUser/AnomalousBehavior` `Impact:IAMUser/AnomalousBehavior` `InitialAccess:IAMUser/AnomalousBehavior` `Persistence:IAMUser/AnomalousBehavior` `PrivilegeEscalation:IAMUser/AnomalousBehavior`	29 mars 2021

Différences supplémentaires pour les AWS GovCloud (US) régions	Detective est désormais disponible dans les AWS GovCloud (US) régions. Aux États-Unis AWS GovCloud (Est des États-Unis) et AWS GovCloud (Ouest des États-Unis), Detective n'envoie pas d'e-mails d'invitation aux comptes des membres. Detective ne supprime pas non plus automatiquement les comptes membres qui sont fermés dans AWS.	24 mars 2021
Ajout d'onglets pour filtrer la liste des comptes membres en fonction du statut des comptes membres	La liste des comptes membres affiche désormais des onglets que vous pouvez utiliser pour filtrer la liste en fonction du statut du compte membre. Vous pouvez consulter tous les comptes membres, ceux dont le statut est Accepté (Activé) ou ceux dont le statut est autre que Accepté (Activé).	16 mars 2021
Ajout de la prise en charge de types de GuardDuty recherche Amazon supplémentaires	Detective propose désormais des profils pour les types de GuardDuty recherche supplémentaires suivants : `Backdoor:EC2/C&CActivity.B` `Impact:EC2/PortSweep` , `Impact:EC2/WinRMBruteForce` , et `PrivilegeEscalation:IAMUser/AdministrativePermissions`	4 mars 2021

Ajout d'une option au script Python pour supprimer les e-mails d'invitation	Le script `enableDetective.py` Detective propose désormais une option `--disable_email` . Lorsque vous incluez cette option, Detective n'envoie pas d'e-mails d'invitation aux comptes membres.	26 février 2021
« Compte principal » est remplacé par « Compte administrateur ».	Le terme « Compte principal » est remplacé par « Compte administrateur ». Le terme est également modifié dans la console Detective et dans l'API.	25 février 2021
« Compte principal » est remplacé par « Compte administrateur »	Le terme « Compte principal » est remplacé par « Compte administrateur ». Le terme est également modifié dans la console Detective et dans l'API.	25 février 2021
Ajout de détails d'activité pour le volet de profil du volume de flux VPC vers et depuis l'adresse IP du résultat	Le volet de profil Volume de flux VPC vers et depuis l'adresse IP du résultat vous permet désormais d'afficher les détails d'activité. Les détails d'activité ne sont disponibles que si le résultat est associé à une seule adresse IP. Les détails d'activité indiquent le volume pour chaque combinaison de ports, de protocole et de direction.	25 février 2021

Ajout d'une option d'API pour ne pas envoyer d'e-mails d'invitation aux comptes membres	Lorsque vous utilisez l'API Detective pour ajouter des comptes membres, les comptes administrateurs peuvent choisir de ne pas envoyer d'e-mails d'invitation aux comptes membres.	25 février 2021
Nouveaux détails d'activité pour le volet de profil du volume global d'appels d'API sur les profils d'adresses IP	Vous pouvez désormais afficher les détails d'activité des adresses IP à partir du volet de profil Volume global d'appels d'API. Les détails d'activité indiquent le nombre d'appels réussis et échoués pour chaque ressource ayant émis l'appel depuis l'adresse IP.	23 février 2021
Nouveau volet de profil de volume global de flux VPC sur les profils d'adresses IP	Le profil d'adresse IP contient désormais le volet de profil de volume global de flux VPC. Le volet de profil indique le volume du trafic de flux VPC à destination et en provenance de l'adresse IP. Vous pouvez afficher les détails de l'activité pour afficher le volume de chaque EC2 instance avec laquelle l'adresse IP a communiqué.	21 janvier 2021

Ajout de la page Récapitulatif Detective	La page Detective Summary contient des visualisations destinées à guider les analystes vers les entités présentant un intérêt en fonction de la géolocalisation, du nombre d'appels d'API et du volume de trafic Amazon EC2 .	21 janvier 2021
Mise à jour de l'option permettant de passer d'Amazon GuardDuty à Detective	Dans GuardDuty, l'option Investigate in Detective est déplacée du menu Actions vers le panneau des détails de la recherche. Elle affiche une liste d'entités associées . Si le type de résultat est pris en charge, la liste inclut également le résultat. Vous pouvez ensuite choisir d'accéder à un profil d'entité ou à un profil de résultat.	15 janvier 2021
Ajout d'une option pour définir la durée de validité par défaut de la fenêtre de détails d'activité	Dans les détails d'activité pour le volume global d'appels d'API et le volume global de flux VPC, vous pouvez définir la fenêtre temporelle pour les détails d'activité sur la durée de validité par défaut du profil.	15 janvier 2021

Ajout de la gestion des intervalles de temps importants pour les entités	Ajout d'un nouvel avis pour indiquer lorsqu'une entité possède un ou plusieurs intervalles de temps élevés. Une nouvelle page d'entités à volume élevé affiche tous les intervalles de volume élevés pour la durée de validité actuelle.	18 décembre 2020
Le quota de comptes membres est passé à 1 200	Les comptes principaux peuvent désormais inviter jusqu'à 1 200 comptes membres à accéder à leur graphe de comportement. Auparavant, le quota était de 1 000.	11 décembre 2020
Valeurs ajoutées pour les quotas de volume de données des graphes de comportement	Les informations sur les quotas de volume de données des graphes de comportement ont été mises à jour afin d'ajouter des valeurs de quota spécifiques.	11 décembre 2020
Ajout de la sélection de la plage de temps pour les détails d'activité dans le volet de profil du volume global d'appels de l'API	Dans le volet Volume global du flux d'API, vous pouvez désormais afficher les détails d'activité pour n'importe quelle plage de temps sélectionnée. Le volet affiche initialement une option permettant d'afficher les détails d'activité pour la durée de validité.	29 septembre 2020

Ajout de la sélection d'intervalles de temps pour les détails d'activité sur le volet de profil de volume global de flux VPC	Dans le volet Volume global de flux VPC, vous pouvez afficher les détails d'activité pour un seul intervalle de temps à partir du graphe. Pour afficher les détails de l'intervalle de temps, choisissez l'intervalle de temps.	25 septembre 2020
Nouvelle session de rôle et entités utilisateur fédérées	Detective vous permet désormais d'explorer et d'étudier l'authentification fédérée. Vous pouvez voir quelles ressources ont assumé chaque rôle et à quel moment ces authentifications ont eu lieu.	17 septembre 2020
Mises à jour de la gestion de la durée de validité	Suppression de l'option permettant de verrouiller ou de déverrouiller la durée de validité. Elle est toujours verrouillée. Sur un profil de résultat, un avertissement s'affiche si la durée de validité est différente de la fenêtre temporelle de résultats.	4 septembre 2020

L'en-tête du profil reste visible lorsque vous parcourez un profil	Sur les profils, le type, l'identifiant et la durée de validité restent visibles lorsque vous parcourez les volets de profil d'un onglet. Lorsque les onglets ne sont pas visibles, vous pouvez utiliser la liste déroulante des pistes de navigation pour accéder à un autre onglet.	4 septembre 2020
La recherche affiche toujours les résultats de recherche	Lorsque vous effectuez une recherche, les résultats s'affichent désormais sur la page Recherche. À partir des résultats, vous pouvez passer à un résultat ou à un profil d'entité.	27 août 2020
Ajouté aux critères autorisés pour les recherches	Les critères autorisés pour les recherches ont été étendus. Vous pouvez rechercher des AWS utilisateurs et AWS des rôles par nom. Vous pouvez utiliser l'ARN pour rechercher des résultats, AWS des rôles, des AWS utilisateurs et des EC2 instances.	27 août 2020

Liens vers d’autres consoles depuis les volets de profil	Dans le EC2 panneau de profil des détails de l' EC2 instance, l'identifiant de l'instance est lié à la EC2 console Amazon. Dans les volets de profil Détails de l’utilisateur et Détails du rôle, le nom d’utilisateur et le nom du rôle sont liés à la console IAM.	14 août 2020
Détails d’activité pour les données de flux VPC	Le volet de profil Volume global de flux VPC permet désormais d’accéder aux détails d’activité. Les détails de l'activité indiquent le flux de trafic entre les adresses IP et une EC2 instance au cours d'une période sélectionnée.	23 juillet 2020
Les comptes membres peuvent désormais voir leur utilisation et leur coût prévisionnel	Les comptes membres peuvent désormais consulter leurs propres informations d’utilisation. Pour les comptes membres, la page Utilisation indique la quantité de données ingérées dans chaque graphe de comportement auquel ils contribuent. Les comptes membres peuvent également consulter leur coût prévu sur 30 jours.	26 mai 2020

L'essai gratuit est désormais par compte plutôt que par graphe de comportement	Chaque compte Amazon Detective bénéficie désormais d'un essai gratuit distinct dans chaque région. L'essai gratuit commence soit lorsque le compte active Detective, soit la première fois que le compte est activé en tant que compte membre.	26 mai 2020
Nouveaux scripts Python open source sur GitHub	Le nouveau amazon-detective-multiaccount-scripts référentiel GitHub fournit des scripts Python open source que vous pouvez utiliser pour gérer les graphes de comportement dans toutes les régions. Vous pouvez activer Detective, ajouter des comptes membres, supprimer des comptes membres et désactiver Detective.	21 janvier 2020
Présentation d'Amazon Detective	Detective utilise le machine learning et des visualisations spécialement conçues pour vous aider à analyser et à étudier les problèmes de sécurité liés à vos charges de travail Amazon Web Services (AWS).	2 décembre 2019

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.