Guide de l’utilisateur

AWS Audit Manager

AWS Audit Manager: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'AWS Audit Manager ? 1
Fonctionnalités d'AWS Audit Manager 1
Tarification pour AWS Audit Manager 3
Vous utilisez pour la première fois Audit Manager ? 3
Ressources AWS Audit Manager supplémentaires 3
Concepts et terminologie 4
A 4
C 6
D 10
E 13
F 16
R 17
S 19
Collecte de preuves 20
Fréquence de collecte des preuves 21
Exemples de contrôles 22
Contrôles automatisés (Security Hub) 23
Contrôles automatisés (AWS Config) 25
Contrôles automatisés (appels d'API) 27
Contrôles automatisés (CloudTrail) 29
Contrôles manuels 31
Contrôles utilisant des sources de données mixtes 33
Intégrations Service AWS 36
Intégrations GRC tierces 37
Comprendre les intégrations tierces 38
Produits GRC tiers pris en charge 39
Utiliser d'Audit Manager avec un SDK AWS 40
Configuration 42
Prérequis 42
S'inscrire à un Compte AWS 42
Création d'un utilisateur administratif 43
Ajoutez les autorisations requises 44
Activer Audit Manager 45
Recommandations 49

Fonctionnalités recommandées 50
Intégrations recommandées 50
Que puis-je faire ensuite ? 56
Mise en route 56
Mettez à jour vos paramètres 56
Démarrer 57
Tutoriels Audit Manager 58
Tutoriel pour les responsables d'audit : création d'une évaluation 58
Étape 1 : Indiquer les détails de l'évaluation 59
Étape 2 : Indiquer les comptes concernés 60
Étape 3 : Indiquer des services concernés 61
Étape 4 : Indiquer les responsables de l'audit 61
Étape 5 : Vérification et création 62
Comment procéder ensuite ? 62
Tutoriel pour les délégués : Vérification d'un ensemble de contrôles 63
Étape 1 : Accéder à vos notifications 64
Étape 2 : Vérifier un ensemble de contrôles et les éléments de preuve 65
Étape 3 : Charger des preuves manuelles 66
Étape 4 : Ajouter un commentaire 67
Étape 5 : Mettre à jour l'état du contrôle 68
Étape 6. Soumettre l'ensemble de contrôle vérifié au responsable de l'audit 68
Comment procéder ensuite ? 69
Utilisation du tableau de bord 70
Concepts et terminologie du tableau de bord 71
Éléments du tableau de bord 74
Filtre d'évaluation 75
Aperçu quotidien 75
Contrôles comportant des preuves non conformes regroupés par domaine de contrôle 76
Que puis-je faire ensuite ? 78
Résolution des problèmes 79
Évaluations 80
Création d'une évaluation 81
Étape 1 : Indiquer les détails de l'évaluation 81
Étape 2 : Indiquer les comptes concernés 83
Étape 3 : Indiquer des services concernés 84
Étape 4 : Indiquer les responsables de l'audit 85

Étape 5 : Vérification et création 86
Que puis-je faire ensuite ? 86
Accéder à une évaluation 87
Modification d'une évaluation 88
Étape 1 : Modifier les détails de l'évaluation 88
Étape 2 : Modifier les comptes concernés 89
Étape 3 : Modifier les services concernés 89
Étape 4 : Modifier les responsables d'audit 90
Étape 5 : Vérification et sauvegarde 91
Vérification d'une évaluation 91
Détails de l'évaluation 92
Onglet Contrôles 93
Onglet de sélection du rapport d'évaluation 94
Onglet Comptes AWS 95
Onglet Services AWS 95
Onglet des responsables de l'Audit 96
Onglet Balises 96
Onglet Journal des modifications 97
Vérification des contrôles d'évaluation 97
Détail du contrôle 98
État du contrôle 98
Onglet Dossiers de preuves 99
Onglet Source de données 100
Onglet des commentaires 101
Onglet Journal des modifications 101
Examiner les éléments probants 102
Examen des dossiers de preuves 102
Examen des preuves individuelles 105
Ajouter des preuves manuelles 107
Comment ajouter des preuves manuelles 108
Formats de fichier pris en charge 117
Génération de rapports d'évaluation 118
Ajouter des preuves 118
Suppression des preuves 120
Génération d'un rapport 121
Que puis-je faire ensuite ? 122

Modifier le statut d'une évaluation 122
Suppression d'une évaluation 124
La délégation 127
Pour les responsables d'audit 127
Délégation d'une série de contrôles 128
Accès aux délégations 130
Supprimer des délégations 131
Pour les délégués 132
Affichage des notifications 133
Examen des contrôles et des éléments probants 133
Ajout de commentaires 135
Marquer un contrôle comme vérifié 136
Renvoi d'une série de contrôles vérifiée au responsable d'audit 136
Rapports d'évaluation 138
Structure du dossier 138
Comment naviguer dans un rapport 138
Sections du rapport 139
Page de couverture 140
Page d'aperçu 140
Page de table des matières 141
Page de contrôle 141
Page récapitulative des preuves 143
Page détaillée des preuves 144
Contrôle de l'intégrité du rapport 144
Résolution des problèmes 145
Outil de recherche d'éléments probants 146
Maîtriser l'outil de recherche d'éléments probants, avec CloudTrail Lake 146
Activation de l'outil de recherche d'éléments probants 148
Résolution des problèmes liés à l'outil de recherche d'éléments probants 148
Recherchez des éléments probants 148
Exécution d'une requête de recherche 148
Interrompre une requête de recherche 150
Modification des filtres de recherche 151
Affichage des résultats dans l'outil de recherche d'éléments probants 152
Affichage des résultats groupés 153
Affichage des résultats de la recherche 154

Options de filtres et de regroupement 161
Référence du filtre 161
Référence de regroupement 166
Exemples de cas d'utilisation 167
Cas d'utilisation 1 : trouver des éléments probants non conformes et organiser des délégations 167
Cas d'utilisation 2 : Identification des preuves de conformité 168
Cas d'utilisation 3 : aperçu rapide des ressources d'éléments probants 169
Centre de téléchargement 171
Naviguer dans le centre de téléchargement 171
Téléchargement d'un fichier 172
Supprimer un fichier 173
Bibliothèque de frameworks 174
Accès à un framework 175
Affichage des détails du framework 176
Création d'un framework personnalisé 180
Créer un nouveau 180
Personnaliser un framework existant 182
Modification d'un framework personnalisé 185
Étape 1 : Spécifier les détails du framework 186
Étape 2 : Modification des contrôles 186
Étape 3. Vérifier et mettre à jour 187
Suppression d'un framework personnalisé 188
Partage d'un framework personnalisé 189
Concepts et terminologie de partage 191
Envoi d'une demande de partage 199
Réponse à une demande de partage 205
Suppression d'une demande de partage 210
Frameworks pris en charge 211
ACSC Essential Eight 212
ACSC ISM 214
Exemple de framework AWS Audit Manager 217
Barrières de protection AWS Control Tower 219
Bonnes pratiques en matière d'IA générative AWS pour Amazon Bedrock 221
AWS License Manager 229
AWSBonnes pratiques de sécurité de base 232

Bonnes pratiques de fonctionnement pour AWS 234
AWS Well-Architected 237
Profil de contrôle du cloud CCCS Medium 239
CIS AWS Foundations Benchmark v.1.2 242
CIS AWS Foundations Benchmark v.1.3 253
CIS AWS Foundations Benchmark v.1.4 257
Contrôles CIS v7.1 IG1 262
Contrôles CIS v8 IG1 265
Référence modérée FedRAMP 268
Règlement général sur la protection des données (RGPD) 271
Loi Gramm-Leach-Bliley 299
GxP 21 CFR partie 11 302
Annexe 11 du GxP EU 305
HIPAA Security Rule 2003 307
HIPAA Final Omnibus Security Rule 2013 311
ISO/IEC 27001:2013 315
NIST 800-53 (Rev. 5) 317
NIST CSF v1.1 321
NIST SP 800-171 (Rev. 2) 324
PCI DSS v3.2.1 327
PCI DSS v4 330
SOC 2 334
Bibliothèque de contrôles 338
Accéder à un contrôle 339
Affichage des détails du contrôle 340
Création d'un contrôle personnalisé 344
Créer un nouveau 345
Personnaliser un framework existant 349
Modification d'un contrôle personnalisé 353
Étape 1 : modifier les détails du contrôle 353
Étape 2 : modifier des sources de données 354
Étape 3 : modifier le plan d'action 355
Étape 4 : Vérifier et mettre à jour 356
Suppression d'un contrôle personnalisé 356
Modification de la fréquence de collecte d'éléments probants 358
Instantanés de configuration issus d'appels d'API 359

Contrôles de conformité effectués par AWS Config 360
Contrôles de conformité effectués par Security Hub 360
Journaux d'activité des utilisateurs provenant de AWS CloudTrail 361
Sources de données de contrôle 361
Sources de données automatisées 362
AWS Config 365
AWS Security Hub 380
AWS Appels d'API 428
AWS CloudTrail 438
Paramètres 440
Paramètres généraux 440
Autorisations 441
Chiffrement des données 441
Administrateur délégué (facultatif) 443
AWS Config (facultatif) 451
Security Hub (facultatif) 451
Désactiver AWS Audit Manager 452
Paramètres d'évaluation 454
Propriétaires de l'audit par défaut (facultatif) 454
Destination du rapport d'évaluation (facultatif) 456
Notifications (facultatif) 459
Paramètres de recherche de preuves 460
Outil de recherche de preuves (facultatif) 461
Destination de l'exportation (facultatif) 467
Notifications 472
Prérequis 472
Configuration des notifications dans AWS Audit Manager 472
Résolution des problèmes 473
Résolution des problèmes 474
Évaluations et collecte de preuves 474
J'ai créé une évaluation, mais je ne vois aucune preuve pour le moment 475
Mon évaluation ne collecte pas de preuves pour la vérification de la conformité auprès d'AWS Security Hub 475
Mon évaluation ne collecte pas de preuves pour la vérification de la conformité auprès d'AWS Config 478

Mon évaluation ne collecte pas de preuves de l'activité des utilisateurs auprès d'AWS CloudTrail 480
Mon évaluation ne collecte pas de preuves de données de configuration pour un appel d'API AWS 480
Mon évaluation ne collecte pas de preuves auprès d'un autre Service AWS 481
Mes preuves sont générées à différents intervalles et je ne sais pas à quelle fréquence elles sont collectées 482
Que se passe-t-il si je supprime un compte concerné de mon organisation ? 483
Je ne parviens pas à modifier les services concernés par mon évaluation 483
Quelle est la différence entre un service concerné et un type de source de données ? 484
Mon évaluation n'a pas pu être créée 485
J'ai désactivé puis réactivé Audit Manager, et à présent, mes évaluations préexistantes ne collectent plus de preuves 485
Rapports d'évaluation 486
Mon rapport d'évaluation n'a pas pu être généré 486
J'ai suivi la liste de contrôle ci-dessus et mon rapport d'évaluation n'a toujours pas été généré 488
Je reçois un message d'erreur d'accès refusé lorsque j'essaie de générer un rapport 488
Je ne suis pas en mesure de décompresser le rapport d'évaluation 489
Lorsque je choisis le nom d'une preuve dans un rapport, je ne suis pas redirigé vers les détails de la preuve 490
La génération de mon rapport d'évaluation est bloquée au statut En cours, et je ne sais pas quelles répercussions cela aura sur ma facturation 490
Voir aussi 490
Contrôles et ensembles de contrôles 491
Je ne vois aucun contrôle ou ensemble de contrôles dans mon évaluation 491
Je ne parviens pas à charger des preuves manuelles dans un contrôle 492
Je dois utiliser plusieurs règles AWS Config comme source de données pour un contrôle unique 492
L'option de règle personnalisée n'est pas disponible pour ma source de données 493
La liste déroulante des règles personnalisées est vide 493
Je ne vois pas la règle personnalisée que je souhaite utiliser 493
Je ne vois pas la règle gérée que je souhaite utiliser 495
Je souhaite partager un cadre personnalisé, mais il comporte des contrôles qui utilisent des règles AWS Config personnalisées comme source de données 498
Que se passe-t-il lorsqu'une règle personnalisée est mise à jour dans AWS Config ? 499

Tableau de bord 500
Mon tableau de bord ne comporte aucune donnée 501
L'option de téléchargement CSV n'est pas disponible 501
Je ne vois pas le fichier téléchargé lorsque j'essaie de télécharger un fichier CSV 501
Un contrôle ou un domaine de contrôle spécifique est absent du tableau de bord 501
L'instantané quotidien affiche des nombres variables de preuves tous les jours. Est-ce normal ? 502
Administrateurs délégués et AWS Organizations 502
Je ne parviens pas à configurer Audit Manager avec mon compte administrateur délégué ... 503
Lorsque je crée une évaluation, je ne parviens pas à voir les comptes de mon organisation sous Comptes concernés 503
Je reçois un message d'erreur accès refusé lorsque j'essaie de générer un rapport d'évaluation à l'aide de mon compte administrateur délégué 504
Que se passe-t-il dans Audit Manager si je dissocie un compte membre de mon organisation ? 505
Que se passe-t-il si je réassocie un compte membre à mon organisation ? 505
Que se passe-t-il si je migre un compte membre d'une organisation vers une autre ? 505
Outil de recherche d'éléments probants 506
Je ne parviens pas à activer l'outil de recherche de preuves 506
J'ai activé l'outil de recherche de preuves, mais je ne vois pas les preuves passées dans mes résultats de recherche 507
Je ne parviens pas à désactiver l'outil de recherche de preuves 507
Ma requête de recherche échoue 508
Je ne parviens pas à générer plusieurs rapports d'évaluation à partir des résultats de ma recherche 511
Je ne parviens pas à inclure des preuves spécifiques à partir des résultats de ma recherche 511
Les résultats de ma recherche de preuves ne sont pas tous inclus dans le rapport d'évaluation 512
Je souhaite générer un rapport d'évaluation à partir des résultats de ma recherche, mais mon instruction de requête échoue 512
Ressources supplémentaires 516
Mon exportation au format CSV a échoué 516
Je ne parviens pas à exporter des preuves spécifiques à partir des résultats de ma recherche 518
Je ne peux pas exporter plusieurs fichiers CSV à la fois 518

Partage de frameworks 519
Le statut de ma demande de partage envoyée s'affiche comme Échec 519
Ma demande de partage est accompagnée d'un point bleu. Qu'est-ce que cela signifie ? 520
Mon cadre partagé comporte des contrôles qui utilisent des règles AWS Config personnalisées comme source de données. Le destinataire peut-il collecter des preuves pour ces contrôles ? 523
J'ai mis à jour une règle personnalisée utilisée dans un cadre partagé. Dois-je prendre des mesures ? 523
Notifications 525
J'ai spécifié une rubrique Amazon SNS dans Audit Manager, mais je ne reçois aucune notification 525
J'ai spécifié une rubrique FIFO, mais je ne reçois pas de notifications dans l'ordre prévu 526
Autorisations et accès 526
J'ai suivi la procédure de configuration d'Audit Manager, mais je n'ai pas suffisamment de privilèges IAM 526
J'ai désigné une personne comme responsable de l'audit, mais elle n'a toujours pas un accès complet à l'évaluation. Pourquoi est-ce le cas ? 527
Je ne parviens pas à exécuter une action dans Audit Manager 527
Je veux autoriser des personnes extérieures à mon Compte AWS à accéder à mes ressources Audit Manager 528
Voir aussi 490
Quotas 530
Quotas par défaut d'Audit Manager 530
Gestion de vos quotas 531
Sécurité 533
Protection des données 534
Suppression des données d'Audit Manager 535
Chiffrement au repos 536
Chiffrement en transit 537
Gestion des clés 537
Gestion des identités et des accès 538
Public ciblé 539
Authentification par des identités 539
Gestion des accès à l'aide de politiques 543
Comment AWS Audit Manager fonctionne avec IAM 546
Exemples de politiques basées sur l'identité 557

Prévention du cas de figure de l'adjoint désorienté entre services 577
AWS politiques gérées 578
Résolution des problèmes 601
Utilisation des rôles liés à un service 603
Validation de conformité 614
Résilience 615
Sécurité de l'infrastructure 616
Points de terminaison d'un VPC (AWS PrivateLink) 616
Considérations relatives aux points de AWS Audit Manager terminaison VPC 617
Création d'un point de terminaison de VPC d'interface pour AWS Audit Manager 617
Création d'une politique de point de terminaison VPC pour AWS Audit Manager 618
Journalisation et surveillance 618
Surveillance avec Amazon EventBridge 619
CloudTrail journaux 623
Configuration et vulnérabilités 627
Balisage de ressources 628
Ressources prises en charge 628
Restrictions liées aux balises 629
Gestion des balises dans Audit Manager 629
Ressources AWS CloudFormation 631
Audit Manager et modèles AWS CloudFormation 631
En savoir plus sur AWS CloudFormation 631
Historique de la documentation 633
Glossaire AWS 646
..... dcxlvii

Qu'est-ce qu'AWS Audit Manager ?

Bienvenue dans le Guide de l'utilisateur d'AWS Audit Manager.

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

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

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

Fonctionnalités d'Audit Manager

AWS Audit Manager vous permet d'effectuer les tâches suivantes :

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

- Chargez et gérez les preuves provenant d'environnements hybrides ou multicloud : outre les preuves collectées par Audit Manager dans votre environnement AWS, vous pouvez également charger et gérer de manière centralisée les preuves issues de votre environnement sur site ou multicloud.
- Prise en charge des normes et réglementations de conformité communes : choisissez l'un des frameworks AWS Audit Manager standard. Ces frameworks fournissent des mappages de contrôle prédéfinis pour les normes et réglementations de conformité communes. Il s'agit notamment des évaluations CIS Foundation, de la norme PCI DSS, du RGPD, de l'HIPAA, du SOC2, de la GxP et des bonnes pratiques opérationnelles d'AWS.
- Surveillez vos évaluations actives : utilisez le tableau de bord d'Audit Manager pour consulter les données analytiques relatives à vos évaluations actives et identifier rapidement les preuves non conformes qui doivent être corrigées.
- Recherchez des preuves : utilisez la fonctionnalité de recherche de preuves pour trouver rapidement des preuves pertinentes pour votre requête de recherche. Vous pouvez générer un rapport d'évaluation à partir de vos résultats de recherche ou les exporter au format CSV.
- Créez des contrôles personnalisés : créez votre propre contrôle à partir de zéro ou personnalisez un contrôle existant pour répondre à vos besoins. Vous pouvez également utiliser la fonctionnalité de contrôles personnalisés pour créer des questions d'évaluation des risques et enregistrer les réponses à ces questions sous forme de preuves manuelles.
- Personnalisation des frameworks : créez vos propres frameworks avec des contrôles standard ou personnalisés en fonction de vos exigences spécifiques en matière d'audits internes.
- Partagez des frameworks personnalisés : partagez vos frameworks personnalisés Audit Manager avec un autre Compte AWS, ou dupliquez-les dans une autre Région AWS dans votre propre compte.
- Prise en charge de la collaboration entre équipes : déléguez les ensembles de contrôle à des experts en la matière qui peuvent examiner les preuves connexes, ajouter des commentaires et mettre à jour le statut de chaque contrôle.
- Créez des rapports pour les auditeurs : générez des rapports d'évaluation qui résument les preuves pertinentes collectées pour votre audit et renvoient à des dossiers contenant les preuves détaillées.
- Garantissez l'intégrité des preuves : stockez les preuves dans un endroit sûr, où elles ne seront pas modifiées.

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

Tarification d'Audit Manager

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

Vous utilisez pour la première fois Audit Manager ?

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

1. AWS Audit Managerconcepts et terminologie d' : découvrez les principaux concepts et termes utilisés dans Audit Manager, tels que les évaluations, les frameworks et les contrôles.
2. De quelle manière AWS Audit Manager collecte les preuves : découvrez comment Audit Manager recueille des preuves pour une évaluation des ressources.
3. Configuration : découvrez les exigences de configuration pour Audit Manager.
4. Mise en route : suivez un tutoriel pour créer votre première évaluation Audit Manager.
5. AWS Audit ManagerRéférence d'API : familiarisez-vous avec les actions et les types de données de l'API Audit Manager.

Plus de ressources concernant Audit Manager

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

- Recueillez des preuves et gérez les données d'audit à l'aide d'AWS Audit Manager
- Configurer manuellement une évaluation personnalisée Audit Manager à partir d'AWS Workshops
- Intégrez dans le modèle à trois lignes (partie 2) : transformez les packs de conformité AWS Config en évaluations AWS Audit Manager, extraites du Blog Gestion & Gouvernance AWS (en anglais)

Concepts et terminologie AWS Audit Manager

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

A

A | B | C | D | E F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Évaluation

Vous pouvez utiliser une évaluation d'Audit Manager pour recueillir automatiquement les preuves pertinentes pour un audit.

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

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

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

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

Rapport d'évaluation

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

Pour en savoir plus sur les rapports d'évaluation, veuillez consulter Rapports d'évaluation. Pour savoir comment générer un rapport d'évaluation, veuillez consulter Génération de rapports d'évaluation.

Destination du rapport d'évaluation

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

Audit

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

Responsable de l'audit

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

Dans le contexte d'Audit Manager, le propriétaire d'un audit est un utilisateur ou un rôle gérant une évaluation et les ressources qui lui sont associées. Les responsabilités de ce persona au sein d'Audit Manager comprennent la création d'évaluations, l'examen des preuves et la génération de rapports d'évaluation. Audit Manager est un service collaboratif, et les propriétaires de l'audit bénéficient de la participation d'autres parties prenantes à leurs évaluations. Par exemple, vous pouvez ajouter d'autres propriétaires d'audit à votre évaluation pour partager les tâches de gestion. Ou bien, si vous êtes propriétaire d'un audit et que vous avez besoin d'aide pour interpréter les preuves recueillies pour un contrôle, vous pouvez déléguer cet ensemble de contrôles à une partie prenante spécialisée dans ce domaine. Une telle personne est connue sous le nom de personne déléguée.

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

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

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

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

C

A | B | C | D | E F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Journal des modifications

Pour chaque contrôle au sein d'une évaluation, Audit Manager capture les journaux des modifications afin de suivre l'activité des utilisateurs relative à ce contrôle. Vous pouvez ensuite consulter une piste d'audit des activités liées à un contrôle spécifique. Pour plus d'informations concernant les activités des utilisateurs enregistrées dans les journaux des modifications, veuillez consulter Onglet Journal des modifications.

Conformité dans le cloud

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

Règlement de conformité

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

Norme de conformité

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

Contrôle

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

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

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

Il existe deux types de contrôle dans Audit Manager :

- Contrôles standard : il s'agit de contrôles prédéfinis associés à un framework spécifique dans Audit Manager. Utilisez les contrôles standard pour vous aider à préparer les audits conformément aux différentes normes et réglementations de conformité.
- Contrôles personnalisés : il s'agit de contrôles personnalisés que vous définissez en tant qu'utilisateur d'Audit Manager. Utilisez les contrôles personnalisés pour vous aider à répondre aux exigences de conformité spécifiques en matière d'audits internes ou d'évaluations des risques liés aux fournisseurs.

Pour plus d'informations, veuillez consulter la section Exemples de contrôles AWS Audit Manager. Pour voir les instructions de création et de gestion des contrôles, veuillez consulter Bibliothèque de contrôles.

Domaines de contrôle

Vous pouvez considérer un domaine de contrôle comme une catégorie générale de contrôles qui n'est pas spécifique à un framework en particulier. Les groupements de domaines de contrôle sont l'une des fonctionnalités les plus puissantes du tableau de bord d'Audit Manager. Audit Manager met en évidence les contrôles de vos évaluations qui contiennent des preuves non conformes et les regroupe par domaine de contrôle. Cela vous permet de concentrer vos efforts de remédiation sur des domaines spécifiques lorsque vous vous préparez à un audit.

> **Note**
>
> Un domaine de contrôle est différent d'un ensemble de contrôles. Un ensemble de contrôles est un regroupement de contrôles spécifique à un framework qui est généralement défini par un organisme de réglementation. Par exemple, le framework PCI DSS possède un ensemble de contrôles nommé Exigence 8 : identifier et authentifier l'accès aux composants du système. Cet ensemble de contrôles relève du domaine de contrôle de la gestion des identités et des accès.

Audit Manager classe les contrôles dans les domaines de contrôle suivants.

Nom du domaine de contrôle	Description de ce que ces contrôles régissent
Continuité des activités et planifica	La manière dont vous établissez des processus protégeant les opération s commerciales critiques des effets des perturbations majeures du système et du réseau.

Nom du domaine de contrôle	Description de ce que ces contrôles régissent
tion des contingences	
Gestion des modifications	La manière dont vous testez, approuvez, implémentez et documentez les modifications apportées à votre infrastructure cloud.
Sécurité et confidentialité des données	La manière dont vous garantissez la confidentialité, la disponibilité et l'intégrité de vos données.
Gestion du développement et de la configuration	La manière dont vous maintenez votre infrastructure cloud dans un état souhaité et constant.
Gouvernance et supervision	La manière dont vous adaptez votre utilisation du cloud computing à vos obligations légales, réglementaires et éthiques.
Gestion des identités et des accès	La manière dont vous garantissez que les bons utilisateurs disposent de l'accès approprié à vos ressources technologiques.
Gestion des incidents	La manière dont vous établissez les responsabilités et les procédures qui garantissent une réponse rapide et efficace aux incidents de sécurité.
Journalisation et surveillance	La manière dont vous examinez l'activité des utilisateurs pour détecter tout signe indiquant qu'une activité non autorisée a été tentée ou exécutée.
Gestion du réseau	La manière dont vous administrez et exploitez votre réseau de données à l'aide d'un système de gestion réseau.
Gestion du personnel	La manière dont vous évaluez et gérez les risques liés à la sécurité du personnel au niveau de l'organisation.

Nom du domaine de contrôle	Description de ce que ces contrôles régissent
Sécurité physique	La manière dont vous détectez et prévenez les problèmes de sécurité physique dans vos installations.
Gestion des risques	La manière dont vous évaluez les risques et les pertes potentiels, et dont vous réduisez ou éliminez ces menaces.
Gestion de la chaîne d'approvisionnement	La manière dont vous identifiez, évaluez et atténuez les risques associés aux produits informatiques, aux fournisseurs et aux chaînes d'approvisionnement.
Gestion des appareils utilisateur	La manière dont vous réduisez le risque de perte, d'endommagement ou de compromission du matériel informatique de vos employés.
Gestion de la vulnérabilité	La manière dont vous définissez, évaluez et corrigez toutes les vulnérabilités connues des actifs de votre infrastructure cloud.

D

A | B | C | D | E F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Source de données

Audit Manager utilise une source de données pour recueillir des preuves en vue d'un contrôle. La terminologie ci-dessous décrit ce qu'est une source de données et son fonctionnement.

- Un type de source de données définit l'endroit depuis lequel Audit Manager recueille les preuves pour un contrôle. Si vous chargez vos propres preuves, le type de source de données est Manuel. Si Audit Manager collecte les preuves pour vous, la source de données peut être de quatre types : AWS Security Hub, AWS Config, AWS CloudTrail, ou appels d'API AWS. L'API Audit Manager désigne un type de source de données en tant que sourceType (singulier) ou controlSources (pluriel).
- Un mappage est un mot clé spécifique associé à un type de source de données. Il peut s'agir, par exemple, d'un nom d'événement CloudTrail ou d'un nom ou AWS Config. L'API Audit Manager y fait référence en tant que sourceKeyword (singulier) ou controlMappingSources (pluriel).

- Un nom de source de données est un nom donné à une source de données. En d'autres termes, le nom d'une source de données indique la combinaison d'un type de source de données et d'un mappage. Concernant les contrôles standard, Audit Manager fournit un nom de source de données par défaut (tel que Source de données 1 et Source de données 2). Concernant les contrôles personnalisés, vous pouvez fournir votre propre nom de source de données. Cela peut vous aider à faire la distinction entre plusieurs sources de données relevant du même type de source de données. L'API Audit Manager fait référence au nom d'une source de données sous le nom de sourceName.

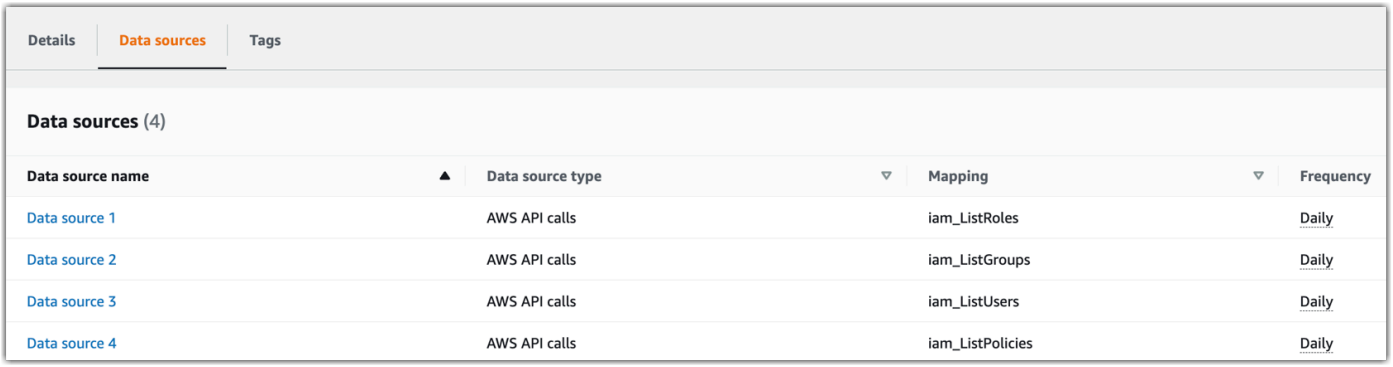
Un seul contrôle peut avoir plusieurs types de sources de données et plusieurs mappages. Par exemple, un contrôle peut recueillir des preuves à partir d'une combinaison de types de sources de données (tels que AWS Config et Security Hub). Un autre contrôle peut avoir AWS Config comme seul type de source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

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

Data source type (Type de source de données)	Description	Exemple de mappage
AWS Security Hub	Utilisez ce type de source de données pour obtenir un instantané de votre niveau de sécurité des ressources. Audit Manager utilise le nom d'un contrôle Security Hub comme mot-clé de mappage et communique le résultat de ce contrôle de sécurité directement depuis Security Hub.	`1.1 – Avoid the use of the "root" account`
AWS Config	Utilisez ce type de source de données pour obtenir un instantané de votre niveau de sécurité des ressource s. Audit Manager utilise	`EC2_INSTANCE_MANAG ED_BY_SSM`

Data source type (Type de source de données)	Description	Exemple de mappage
	le nom d'une règle AWS Config comme mot-clé de mappage et communique le résultat de ce contrôle de règle directement depuis AWS Config.	
AWS CloudTrail	Utilisez ce type de source de données pour suivre une activité utilisateur spécifiqu e nécessaire à votre audit. Audit Manager utilise le nom d'un événement CloudTrail comme mot-clé de mappage et recueille l'activité utilisate ur associée à partir de vos journaux CloudTrail.	`CreateAccessKey`
Appels d'API AWS	Utilisez ce type de source de données pour prendre un instantané de la configura tion de vos ressources à l'aide d'un appel d'API à un Service AWS spécifique. Audit Manager utilise le nom de l'appel d'API comme mot-clé de mappage et recueille la réponse de l'API.	`ec2_DescribeSecuri tyGroups`

L'image suivante montre des exemples de différentes sources de données telles qu'elles apparaissent dans la console d'Audit Manager.



> **Note**
>
> Bien que certains types de sources de données soient des Services AWS, un type de source de données est différent de celui d'un service inclus. Pour plus d'informations, veuillez consulter Quelle est la différence entre un service inclus et un type de source de données ? dans la section Dépannage de ce guide.

Délégué

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

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

E

A | B | C | D | E F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Eléments probants

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

Il existe deux principaux types de preuves dans Audit Manager : les preuves automatisées et les preuves manuelles.

- Preuves automatisées : il s'agit des preuves recueillies automatiquement par Audit Manager. Elles comprennent les trois catégories de preuves automatisées suivantes :
  - Contrôle de conformité : le résultat d'un contrôle de conformité est capturé à partir d'AWS Security Hub, de AWS Config, ou des deux. Parmi les exemples de contrôles de conformité, citons le résultat d'un contrôle de sécurité effectué par Security Hub pour un contrôle PCI DSS et une évaluation des règles AWS Config pour un contrôle HIPAA. Pour plus d'informations, veuillez consulter AWS ConfigRègles prises en charge par AWS Audit Manager et contrôles AWS Security Hub pris en charge par AWS Audit Manager.
  - Activité utilisateur : l'activité utilisateur modifiant la configuration d'une ressource est capturée à partir des journaux CloudTrail au fur et à mesure que cette activité se produit. Des exemples d'activités des utilisateurs comprennent une mise à jour de la table de routage, une modification des paramètres de sauvegarde d'une instance Amazon RDS et une modification de la politique de chiffrement des compartiments S3. Pour plus d'informations, veuillez consulter les noms d'événements AWS CloudTrail pris en charge par AWS Audit Manager.
  - Données de configuration : un instantané de la configuration des ressources est capturé directement à partir d'un Service AWS sur une base quotidienne, hebdomadaire ou mensuelle. Des exemples d'instantanés de configuration comprennent une liste de routes pour une table de routage VPC, un paramètre de sauvegarde d'instance Amazon RDS et une politique de chiffrement des compartiments S3. Pour plus d'informations, veuillez consulter la section appels d'API pris en charge par AWS Audit Manager.
- Preuves manuelles : il s'agit des preuves que vous ajoutez vous-même à Audit Manager. Vous pouvez ajouter vos propres preuves de trois manières :
  - Importer un fichier à partir d'Amazon S3
  - Charger un fichier à partir de votre navigateur
  - Saisir une réponse textuelle à une question d'évaluation des risques

  Pour de plus amples informations, veuillez consulter Ajouter des preuves manuelles dans AWS Audit Manager.

La collecte automatisée de preuves débute lorsque vous créez une évaluation. Il s'agit d'un processus continu, et Audit Manager recueille des preuves à différentes fréquences en fonction du type de preuves et de la source de données sous-jacente. Pour en savoir plus sur la collecte de preuves, veuillez consulter De quelle façon AWS Audit Manager recueille les preuves. Pour obtenir des instructions sur la façon d'examiner les preuves dans une évaluation, veuillez consulter Examen des preuves dans le cadre d'une évaluation.

Méthode de collecte de preuves

Un contrôle peut recueillir des preuves de deux manières.

- Les contrôles automatisés recueillent automatiquement des preuves à partir de sources de données AWS. Ces preuves automatisées peuvent vous aider à démontrer la conformité totale ou partielle envers le contrôle.
- Les contrôles manuels nécessitent que vous chargiez vos propres preuves pour démontrer la conformité envers le contrôle.

> **Note**
>
> Vous pouvez joindre des preuves manuelles à tout contrôle automatisé. Dans de nombreux cas, il est nécessaire d'avoir une combinaison de preuves automatisées et manuelles pour démontrer la conformité totale envers un contrôle. Bien qu'Audit Manager puisse fournir des preuves automatisées utiles et pertinentes, certaines preuves automatisées peuvent ne démontrer qu'une conformité partielle. Dans ce cas, vous pouvez compléter les preuves automatisées fournies par Audit Manager avec vos propres preuves.
>
> Par exemple :
>
> - Le framework des bonnes pratiques en matière d'IA générative d'AWS contient un contrôle appelé `Error analysis`. Ce contrôle vous oblige à identifier les cas de détection d'inexactitudes dans l'utilisation de votre modèle. Cela vous oblige également à effectuer une analyse approfondie des erreurs afin d'en comprendre les causes profondes et d'entreprendre des mesures correctives.
> - Pour prendre en charge ce contrôle, Audit Manager recueille des preuves automatisées qui indiquent si les alarmes CloudWatch sont activées pour l'Compte AWS où votre évaluation est en cours d'exécution. Vous pouvez utiliser ces preuves pour démontrer une conformité partielle avec le contrôle en prouvant que vos alarmes et contrôles sont configurés correctement.

- Pour démontrer une conformité totale, vous pouvez compléter les preuves automatisées avec des preuves manuelles. Par exemple, vous pouvez charger une politique ou une procédure qui indique votre processus d'analyse des erreurs, vos seuils pour les escalades et les rapports, ainsi que les résultats de votre analyse des causes profondes. Vous pouvez utiliser ces preuves manuelles pour démontrer que les politiques établies sont en place et que des mesures correctives ont été prises lorsque cela vous a été demandé.

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

Destination d'exportation

Une destination d'exportation est le compartiment S3 par défaut dans lequel Audit Manager enregistre les fichiers que vous exportez depuis la recherche de preuves. Pour en savoir plus, veuillez consulter la section Destination de l'exportation (facultatif).

F

A | B | C | D | E F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Framework

Un framework Audit Manager est un fichier utilisé pour structurer et automatiser les évaluations relatives à une norme donnée ou à un principe de gouvernance des risques. Ces frameworks permettent de faire correspondre vos ressources AWS aux exigences d'un contrôle. Ils comprennent un ensemble de contrôles prédéfinis ou définis par le client. Celui-ci contient des descriptions et des procédures de test pour chaque contrôle. Ces contrôles sont organisés et regroupés en fonction des exigences de la norme ou de la réglementation de conformité spécifiée. Des exemples incluent les normes PCI DSS et le RGPD.

Il existe deux types de frameworks dans Audit Manager :

- Frameworks standard : les frameworks prédéfinis sont basés sur les bonnes pratiques AWS relatives aux différentes normes et réglementations de conformité. Vous pouvez utiliser ces frameworks pour vous aider à préparer votre audit.
- Frameworks personnalisés : frameworks personnalisés que vous définissez en tant qu'utilisateur d'Audit Manager. Vous pouvez utiliser ces frameworks pour vous aider à

préparer les audits conformément à vos exigences spécifiques en matière de conformité ou de gouvernance des risques.

Pour voir les instructions de création et de gestion des frameworks, veuillez consulter Bibliothèque de frameworks.

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

Partage de frameworks

Vous pouvez utiliser la fonctionnalité de partage de frameworks personnalisés d'Audit Manager pour partager rapidement vos frameworks personnalisés entre des Comptes AWS et des régions. Pour partager un framework personnalisé, vous devez créer une demande de partage. Le destinataire de la demande de partage dispose alors de 120 jours pour accepter ou refuser la demande. Lorsqu'il accepte la demande de partage, Audit Manager reproduit le framework personnalisé partagé dans sa bibliothèque de frameworks. Outre la réplication du framework personnalisé, Audit Manager reproduit également tous les ensembles de contrôles personnalisés et les contrôles personnalisés contenus dans ce framework. Ces contrôles personnalisés sont ajoutés à la bibliothèque de contrôles du destinataire. Audit Manager ne réplique pas les frameworks ou les contrôles standard. Cela est dû au fait que ces ressources sont déjà disponibles par défaut dans chaque compte et région.

R

A | B | C | D | E F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Ressource

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

Évaluation des ressources

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

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

Conformité des ressources

La conformité des ressources fait référence au statut d'évaluation d'une ressource qui a été évaluée lors du recueil de preuves pour la vérification de conformité.

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

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

Dans la recherche de preuves, il existe trois valeurs possibles pour la conformité des ressources :

- Non conforme : il s'agit de ressources présentant des problèmes au niveau de la vérification de conformité. Cela se produit si Security Hub signale un résultat d'échec pour la ressource ou si AWS Config signale un résultat non conforme.
- Conforme : il s'agit de ressources ne présentant pas de problèmes au niveau de la vérification de conformité. Cela se produit si Security Hub signale un résultat de réussite pour la ressource ou si AWS Config signale un résultat conforme.
- Non concluant : il s'agit de ressources pour lesquelles aucune vérification de conformité n'est disponible ou applicable. Cela se produit si AWS Config ou Security Hub constituent le type de source de données sous-jacent, mais que ces services ne sont pas activés. Cela se produit également si le type de source de données sous-jacent ne prend pas en charge les vérifications de conformité (tels que les preuves manuelles, les appels d'API AWS ou CloudTrail).

S

A | B | C | D | E F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Service inclus

Il s'agit d'un Service AWS qui est inclus dans la portée de votre évaluation. Lorsque vous spécifiez un service comme étant inclus dans la portée de votre évaluation, Audit Manager évalue les ressources de ce service. Audit Manager peut évaluer une grande variété de ressources provenant d'un service inclus. Quelques exemples de ressources possibles :

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

Lorsque vous utilisez la console Audit Manager pour créer ou mettre à jour une évaluation à partir d'un framework standard, la liste des Services AWS concernés est présélectionnée. Cette liste ne peut pas être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework standard. S'il s'agit d'un framework standard qui ne contient que des contrôles manuels, aucun Services AWS n'est concerné par votre évaluation et vous ne pouvez lui ajouter aucun service.

Si vous devez modifier la liste des services concernés par un framework standard, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

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

De quelle façon AWS Audit Manager recueille les preuves

Chaque évaluation active d'AWS Audit Manager recueille automatiquement des preuves à partir de diverses sources de données. Chaque évaluation a une portée définie qui spécifie les Services AWS et les comptes à partir desquels Audit Manager recueille les données. Chacun de ces services et comptes définis dans le champ d'application contient plusieurs ressources, et chaque ressource constitue un inventaire des actifs du système dont vous êtes le propriétaire. La collecte de preuves dans Audit Manager implique l'évaluation de chaque ressource concernée. C'est ce que l'on appelle une évaluation des ressources.

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

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

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

2. Conversion des résultats d'évaluation en preuves

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

3. Lien des preuves au contrôle correspondant

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

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

Fréquence de collecte des preuves

La collecte de preuves est un processus continu qui commence lorsque vous créez votre évaluation. AWS Audit Manager recueille des preuves provenant de plusieurs sources de données à des fréquences variables. Par conséquent, il n'existe pas de réponse universelle quant à la fréquence à laquelle les preuves sont collectées. La fréquence de collecte des preuves est basée sur le type de preuve et sa source de données, comme décrit ci-dessous.

- Contrôles de conformité : Audit Manager recueille ce type de preuves auprès de AWS Security Hub et de AWS Config.
  - Pour AWS Security Hub, la fréquence de collecte des preuves suit le calendrier des vérifications de votre Security Hub. Pour plus d'informations sur le calendrier des vérifications du Security Hub, veuillez consulter la section Planification de l'exécution des contrôles de sécurité dans le Guide de l'utilisateur AWS Security Hub. Pour plus d'informations sur les vérifications de Security Hub pris en charge par Audit Manager, veuillez consulter AWS Security Hub commandes prises en charge par AWS Audit Manager.
  - Concernant AWS Config, la fréquence de collecte des preuves suit les déclencheurs définis dans vos règles AWS Config. Pour plus d'informations sur les déclencheurs des règles AWS Config, veuillez consulter la section Types de déclencheurs dans le Guide de l'utilisateur AWS Config. Pour plus d'informations sur les AWS Config Rules pris en charge par Audit Manager, veuillez consulter AWS Config Rules soutenu par AWS Audit Manager.
- Activité utilisateur : Audit Manager collecte ce type de preuves à partir de AWS CloudTrail de manière continue. Cette fréquence est continue car l'activité utilisateur peut se produire à tout moment de la journée. Pour de plus amples informations, veuillez consulter AWS CloudTrail noms d'événements pris en charge par AWS Audit Manager.

- Données de configuration : Audit Manager recueille ce type de preuve à l'aide d'un appel d'API de description à un autre Service AWS tel qu'Amazon EC2, Amazon S3 ou IAM. Vous pouvez choisir quelles actions d'API appeler. Vous pouvez également définir la fréquence sur quotidienne, hebdomadaire ou mensuelle dans Audit Manager. Vous pouvez la spécifier lorsque vous créez ou modifiez un contrôle dans la bibliothèque de contrôles. Pour voir les instructions d'édition et de création des contrôles, veuillez consulter Bibliothèque de contrôles. Pour plus d'informations sur la manière dont Audit Manager utilise les appels d'API pour créer des preuves, veuillez consulter Appels d'API pris en charge par AWS Audit Manager.

Quelle que soit la fréquence de collecte des preuves pour la source de données, les nouvelles preuves sont recueillies automatiquement tant que le contrôle et l'évaluation sont actifs.

Exemples de contrôles AWS Audit Manager

Sur cette page, vous pouvez consulter des exemples pour en découvrir plus sur le fonctionnement des contrôles dans AWS Audit Manager. Ces exemples décrivent à quoi ressemble un contrôle, comment Audit Manager génère des preuves pour celui-ci, ainsi que les prochaines étapes à suivre pour démontrer la conformité.

> **Tip**
>
> Nous vous recommandons vivement d'activer AWS Config et AWS Security Hub pour une expérience optimale dans Audit Manager. Lorsque vous activez ces services, ils peuvent être utilisés comme type de source de données pour les contrôles dans le cadre de vos évaluations d'Audit Manager. En d'autres termes, Audit Manager peut utiliser les résultats de Security Hub et de AWS Config Rules pour générer des preuves automatisées.
>
> - Une fois que vous avez activé AWS Security Hub, assurez-vous d'activer également toutes les normes de sécurité et d'activer le paramètre des résultats de contrôle consolidés. Cette étape permet à Audit Manager d'importer les résultats correspondant à toutes les normes de conformité prises en charge.
> - Après l'activation de AWS Config, assurez-vous d'activer également les AWS Config Rules pertinents ou de déployer un pack de conformité pour la norme de conformité associée à votre audit. Cette étape permet à Audit Manager d'importer les résultats des AWS Config Rules pris en charge que vous avez activés.

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

Rubriques

- Contrôles automatisés utilisant AWS Security Hub comme type de source de données
- Contrôles automatisés utilisant AWS Config comme type de source de données
- Contrôles automatisés utilisant des appels d'API AWS comme type de source de données
- Contrôles automatisés utilisant AWS CloudTrail comme type de source de données
- Contrôles manuels
- Contrôles utilisant des types de sources de données mixtes (automatisées et manuelles)

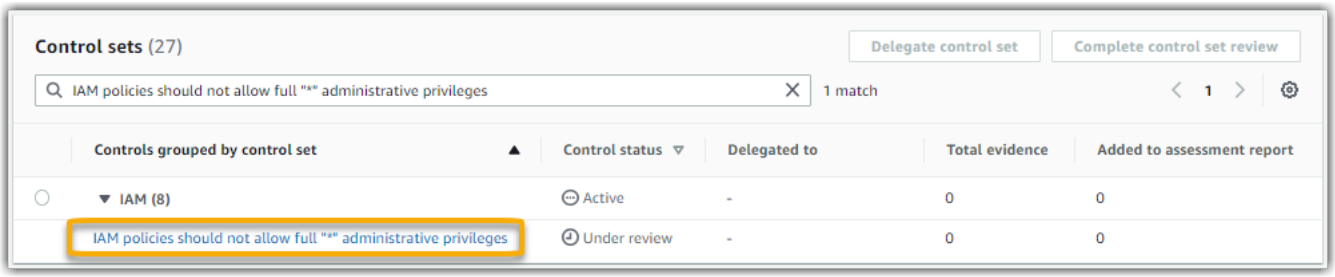
Contrôles automatisés utilisant AWS Security Hub comme type de source de données

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

Exemple de détails de contrôle

- Nom du contrôle : `IAM policies should not allow full "*" administrative privileges`
- Ensemble de contrôles : ce contrôle appartient à l'ensemble de contrôles `IAM`. Il s'agit d'un groupe de contrôles liés à la gestion des identités et des accès.
- Type de source de données : AWS Security Hub
- Type de preuve : vérification de conformité

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



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

Ce que réalise ce contrôle

Audit Manager peut utiliser ce contrôle pour vérifier si vos politiques IAM sont trop larges pour répondre aux exigences du FSBP. Plus précisément, il peut vérifier si les politiques IAM gérées par le client disposent d'un accès administrateur comprenant l'instruction générique suivante : `"Effect": "Allow"` avec `"Action": "*"` sur `"Resource": "*"`.

Fonctionnement de la collecte des preuves par Audit Manager pour ce contrôle

Audit Manager prend les mesures suivantes pour recueillir les preuves pour ce contrôle :

1. Pour chaque contrôle, Audit Manager évalue vos ressources concernées. Pour ce faire, il utilise la source de données spécifiée dans les paramètres de contrôle. Dans cet exemple, vos politiques IAM sont la ressource, et Security Hub et AWS Config sont le type de source de données. Audit Manager recherche le résultat d'une vérification spécifique du Security Hub ([IAM.1]), qui utilise à son tour une règle AWS Config pour évaluer vos politiques IAM (iam-policy-no-statements-with-admin-access).
2. Le résultat de l'évaluation des ressources est enregistré et converti en preuves conviviales pour l'auditeur. Audit Manager génère des preuves pour la vérification de conformité pour les contrôles qui utilisent Security Hub comme type de source de données. Ces preuves contiennent le résultat de la vérification de conformité signalé directement depuis Security Hub.
3. Audit Manager joint les preuves enregistrées au contrôle nommé `IAM policies should not allow full "*" administrative privileges` dans votre évaluation.

Comment utiliser Audit Manager pour démontrer la conformité à ce contrôle

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

Dans cet exemple, Audit Manager peut afficher une décision d'échec émanant de Security Hub. Cela peut se produire si vos politiques IAM contiennent des caractères génériques (*) et sont trop larges pour répondre au contrôle. Dans ce cas, vous pouvez mettre à jour vos politiques IAM afin qu'elles n'accordent pas de privilèges administratifs complets. Pour ce faire, vous pouvez déterminer

quelles tâches doivent effectuer les utilisateurs, puis élaborer des stratégies leur permettant de réaliser uniquement ces tâches. Cette action corrective permet de mettre votre environnement AWS en conformité avec les exigences du FSBP.

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

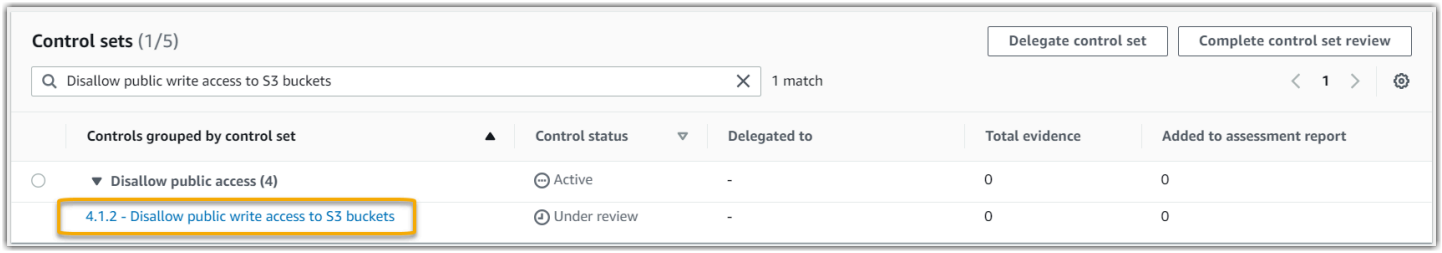
Contrôles automatisés utilisant AWS Config comme type de source de données

Cet exemple montre un contrôle utilisant AWS Config comme type de source de données. Il s'agit d'un contrôle standard issu du framework de barrière de protection AWS Control Tower. Audit Manager utilise ce contrôle pour générer des preuves qui peuvent aider à mettre votre environnement AWS en conformité avec la barrière de protection AWS Control Tower.

Exemple de détails de contrôle

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

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



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

Ce que réalise ce contrôle

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

Fonctionnement de la collecte des preuves par Audit Manager pour ce contrôle

Audit Manager prend les mesures suivantes pour recueillir les preuves pour ce contrôle :

1. Pour chaque contrôle, Audit Manager évalue vos ressources concernées à l'aide de la source de données spécifiée dans les paramètres du contrôle. Dans ce cas, vos compartiments S3 constituent la ressource et AWS Config est le type de source de données. Audit Manager recherche le résultat d'une règle AWS Config spécifique (s3-bucket-public-write-prohibited) afin d'évaluer les paramètres, la politique et l'ACL de chacun des compartiments S3 concernés par votre évaluation.
2. Le résultat de l'évaluation des ressources est enregistré et converti en preuves conviviales pour l'auditeur. Audit Manager génère des preuves de vérification de conformité pour les contrôles qui utilisent AWS Config comme type de source de données. Ces preuves contiennent le résultat de la vérification de conformité signalé directement depuis AWS Config.
3. Audit Manager joint les preuves enregistrées au contrôle nommé `4.1.2 - Disallow public write access to S3 buckets` dans votre évaluation.

Comment utiliser Audit Manager pour démontrer la conformité à ce contrôle

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

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

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

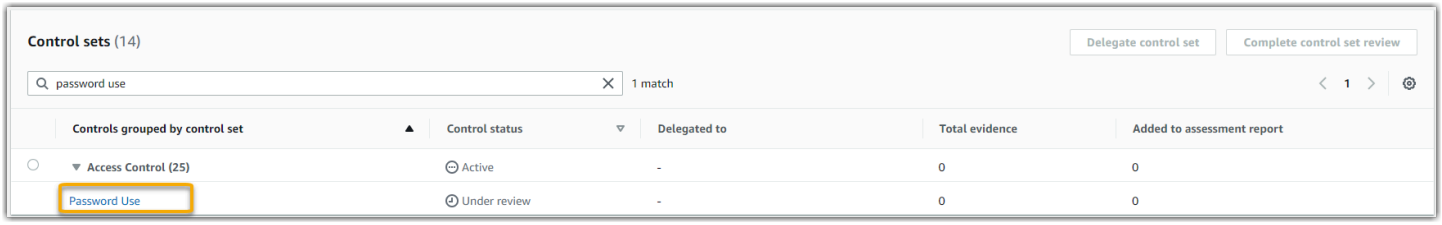
Contrôles automatisés utilisant des appels d'API AWS comme type de source de données

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

Exemple de détails de contrôle

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

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



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

Ce que réalise ce contrôle

Audit Manager peut utiliser ce contrôle personnalisé pour vous aider à garantir que vous avez mis en place des politiques de contrôle d'accès suffisantes. Il nécessite que vous suiviez les bonnes

pratiques de sécurité lors de la sélection et de l'utilisation des mots de passe. Audit Manager peut vous aider à le valider en récupérant une liste de toutes les politiques de mot de passe pour les principaux IAM concernés par votre évaluation.

Fonctionnement de la collecte des preuves par Audit Manager pour ce contrôle

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

1. Pour chaque contrôle, Audit Manager évalue vos ressources concernées à l'aide de la source de données spécifiée dans les paramètres du contrôle. Dans ce cas, vos principaux IAM constituent les ressources, et les appels d'API AWS sont le type de source de données. Audit Manager recherche le résultat d'un appel d'API IAM spécifique (GetAccountPasswordPolicy). Il renvoie ensuite les politiques relatives aux mots de passe pour les Comptes AWS qui entrent dans le cadre de votre évaluation.
2. Le résultat de l'évaluation des ressources est enregistré et converti en preuves conviviales pour l'auditeur. Audit Manager génère des preuves de données de configuration pour les contrôles qui utilisent des appels d'API en tant que source de données. Ces preuves contiennent les données d'origine capturées à partir des réponses de l'API, ainsi que des métadonnées supplémentaires indiquant le contrôle pris en charge par les données.
3. Audit Manager joint les preuves enregistrées au contrôle personnalisé nommé `Password Use` dans votre évaluation.

Comment utiliser Audit Manager pour démontrer la conformité à ce contrôle

Une fois les preuves jointes au contrôle, vous (ou un délégué de votre choix) pouvez les examiner pour déterminer si elles sont suffisantes ou si des mesures correctives sont nécessaires.

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

Lorsque vous êtes certain que les politiques de mots de passe de vos principaux IAM sont conformes au contrôle personnalisé, vous pouvez marquer le contrôle comme examiné et ajouter les preuves

à votre rapport d'évaluation. Vous pouvez ensuite partager ce rapport avec les auditeurs pour démontrer que le contrôle fonctionne comme prévu.

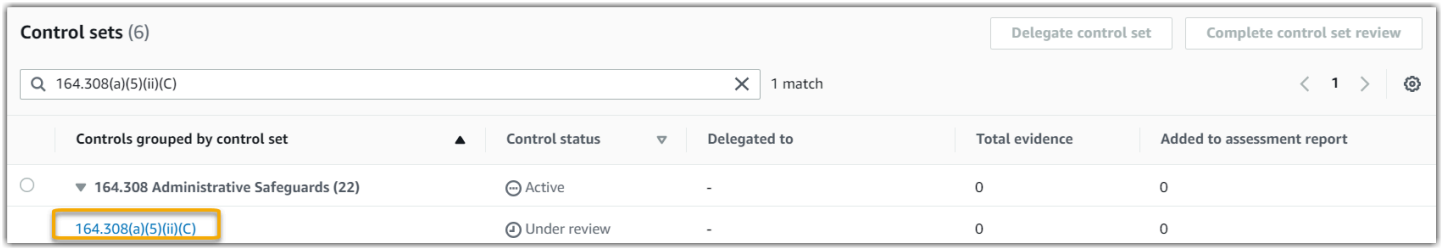
Contrôles automatisés utilisant AWS CloudTrail comme type de source de données

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

Exemple de détails de contrôle

- Nom du contrôle : `164.308(a)(5)(ii)(C)`
- Ensemble de contrôles : ce contrôle appartient à l'ensemble de contrôles appelé `164.308 Administrative Safeguards`.
- Type de source de données : AWS CloudTrail
- Type de preuves : activité utilisateur

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



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

Ce que réalise ce contrôle

Ce contrôle nécessite une procédure de surveillance pour détecter les connexions inappropriées. Par exemple, une connexion inappropriée se produit lorsqu'une personne saisit plusieurs combinaisons

de noms d'utilisateur ou de mots de passe pour tenter d'accéder à un système d'information. Audit Manager vous aide à valider ce contrôle en fournissant une liste de toutes les tentatives de connexion détectées pour les ressources concernées par votre évaluation.

Fonctionnement de la collecte des preuves par Audit Manager pour ce contrôle

Audit Manager prend les mesures suivantes pour recueillir les preuves pour ce contrôle :

1. Pour chaque contrôle, Audit Manager évalue vos ressources concernées à l'aide de la source de données spécifiée dans les paramètres du contrôle. Dans ce cas, vos utilisateurs constituent la ressource et CloudTrail est le type de source de données. Audit Manager recherche le résultat de tous les événements de connexion à la console de gestion AWS enregistrés par CloudTrail. Il renvoie ensuite un journal des événements pertinents entrant dans le cadre de votre évaluation.
2. Le résultat de l'évaluation des ressources est enregistré et converti en preuves conviviales pour l'auditeur. Audit Manager génère des preuves d'activité utilisateur pour les contrôles qui utilisent CloudTrail comme type de source de données. Ces preuves contiennent les données d'origine capturées à partir de vos utilisateurs, ainsi que des métadonnées supplémentaires indiquant le contrôle pris en charge par les données.
3. Audit Manager joint les preuves enregistrées au contrôle nommé `164.308(a)(5)(ii)(C)` dans votre évaluation.

Comment utiliser Audit Manager pour démontrer la conformité à ce contrôle

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

Dans cet exemple, vous pouvez examiner les preuves pour voir les événements de connexion enregistrés par CloudTrail. Ce journal décrit l'activité de connexion de vos utilisateurs à la console, notamment les informations suivantes :

- Chaque connexion réussie
- Chaque tentative de connexion infructueuse
- Vérification du moment où l'authentification multifactorielle (MFA) a été appliquée
- L'adresse IP de chaque événement de connexion

Vous pouvez utiliser ce journal comme preuve pour démontrer que vous avez mis en place des politiques de surveillance suffisantes pour les Comptes AWS concernés par votre évaluation. Si

vous le souhaitez, vous pouvez également fournir des commentaires supplémentaires en ajoutant un commentaire au contrôle. Par exemple, si le journal présente des anomalies, par exemple de multiples tentatives de connexion infructueuses, vous pouvez ajouter un commentaire décrivant la manière dont vous avez résolu le problème. La surveillance régulière des connexions à la console vous aide à prévenir les problèmes de sécurité pouvant découler de divergences ou de tentatives de connexion inappropriées. À son tour, cette bonne pratique contribue à mettre votre environnement AWS en conformité avec les exigences de HIPAA.

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

Contrôles manuels

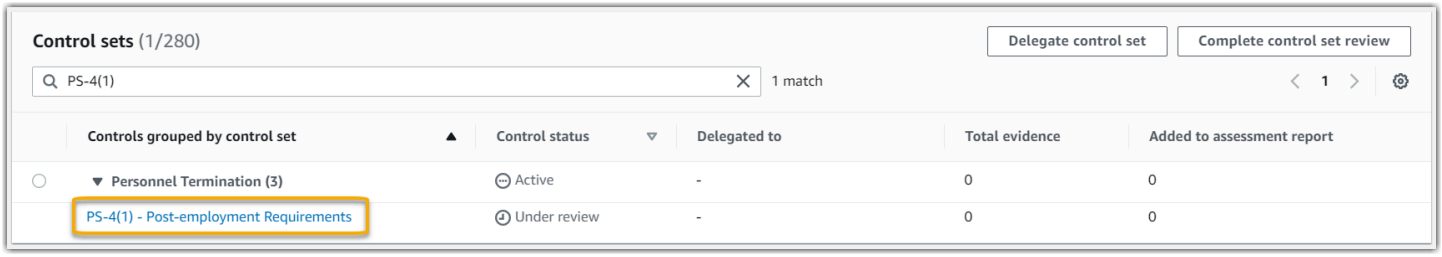
Certains contrôles ne prennent pas en charge la collecte automatisée de preuves. Cela inclut les contrôles qui reposent sur la fourniture d'enregistrements physiques et de signatures, en plus des observations, des entretiens et d'autres événements qui ne sont pas générés dans le cloud. Dans ces cas,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

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

Exemple de détails de contrôle

- Nom du contrôle : `PS-4(1) - Post-employment Requirements`
- Ensemble de contrôles : ce contrôle appartient à l'ensemble de contrôles `Personnel Termination`. Il s'agit d'un ensemble de contrôles relatifs à la sécurité de l'information dans le contexte des procédures de licenciement.
- Type de source de données : manuel
- Type de preuves : manuel

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



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

Ce que réalise ce contrôle

Vous pouvez utiliser ce contrôle pour confirmer que vous protégez les informations de l'organisation en cas de licenciement d'un employé. Plus précisément, vous pouvez démontrer que vous informez systématiquement les personnes licenciées des exigences applicables et juridiquement contraignantes relatives à la protection des informations organisationnelles suivant la fin du contrat. De plus, vous pouvez démontrer que toutes les personnes licenciées signent un accusé de réception des exigences relatives à la période suivant la fin du contrat dans le cadre du processus de licenciement de votre organisation.

Comment charger manuellement des preuves pour ce contrôle

Vous pouvez suivre les étapes suivantes pour charger des preuves manuelles à l'appui de ce contrôle :

1. Placez les preuves manuelles que vous souhaitez charger dans un compartiment Amazon Simple Storage Service (S3) et notez l'URI du S3.
2. Dans votre évaluation Audit Manager, ouvrez le contrôle, accédez à l'onglet des dossiers de preuves et chargez les preuves en saisissant l'URI du S3. Pour obtenir des instructions, veuillez consulter la section Charger des preuves manuelles dans AWS Audit Manager.
3. Audit Manager crée un dossier de preuves nommé d'après la date à laquelle vous les avez chargées. Il joint alors les preuves chargées au contrôle nommé `PS-4(1) - Post-employment Requirements` dans votre évaluation.

Comment utiliser Audit Manager pour démontrer la conformité à ce contrôle

Si vous disposez d'une documentation à l'appui de ce contrôle, vous pouvez la charger sous forme de preuve manuelle. Par exemple, vous pouvez charger la dernière copie des exigences juridiquement contraignantes relatives à la période suivant la fin de contrat que votre service des ressources humaines délivre aux employés licenciés. Si des personnes ont été licenciées pendant la période d'audit, vous pouvez également charger des copies datées adressées à ces personnes licenciées.

Tout comme pour les contrôles automatisés, vous pouvez déléguer des contrôles manuels aux parties prenantes qui peuvent vous aider à examiner les preuves (ou, dans ce cas, à les fournir). Par exemple, lorsque vous passez en revue ce contrôle, vous constaterez peut-être que vous ne répondez que partiellement à ses exigences. Cela peut être le cas si vous n'avez pas de lettre d'accusé de réception signée par une personne licenciée. Vous pouvez déléguer le contrôle à une partie prenante des ressources humaines, qui pourra ensuite charger une copie de la lettre signée. Ou, si aucun employé n'a été licencié pendant la période d'audit, vous pouvez laisser un commentaire expliquant pourquoi aucune lettre signée n'est jointe au contrôle.

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

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

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

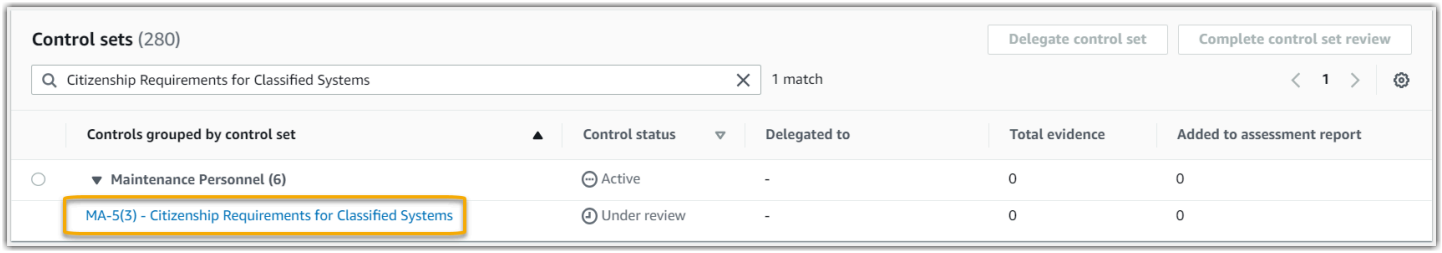
Cet exemple montre un contrôle qui utilise une combinaison de preuves manuelles et automatisées provenant d'appels d'API AWS. Il s'agit d'un contrôle standard issu du framework NIST 800-53 (rév. 5). Audit Manager utilise ce contrôle pour générer des preuves qui peuvent aider à mettre votre environnement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

Exemple de détails de contrôle

- Nom du contrôle : `MA-5(3) - Citizenship Requirements for Classified Systems`
- Ensemble de contrôles : ce contrôle appartient à l'ensemble de contrôles `Maintenance Personnel`. Il s'agit d'un groupe de contrôles relatifs aux personnes qui effectuent la maintenance du matériel ou des logiciels sur les systèmes organisationnels.

- Type de source de données : appels d'API AWS, plus preuves manuelles supplémentaires
- Type de preuves : données de configuration

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



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

Ce que réalise ce contrôle

Audit Manager peut utiliser ce contrôle pour vous aider à garantir que le personnel chargé de vos activités de maintenance et de diagnostic possède le statut de citoyenneté requis. Si votre système traite, stocke ou transmet des informations classifiées, vous devez démontrer que votre personnel de maintenance est composé de citoyens américains. Audit Manager vous aide à valider ce point. Pour ce faire, il renvoie une liste complète des politiques et principaux IAM inclus dans le cadre de votre évaluation. Vous pouvez ensuite vérifier et démontrer que cette liste d'utilisateurs répond aux exigences de citoyenneté nécessaires. Vous pouvez le faire en chargeant manuellement des preuves supplémentaires de leur statut de citoyenneté.

Fonctionnement de la collecte des preuves par Audit Manager pour ce contrôle

Audit Manager prend les mesures suivantes pour recueillir les preuves pour ce contrôle :

1. Pour chaque contrôle, Audit Manager évalue vos ressources concernées à l'aide de la source de données spécifiée dans les paramètres du contrôle. Dans ce cas, vos politiques et principaux IAM constituent les ressources, et les appels d'API AWS sont le type de source de données. Audit Manager recherche le résultat de quatre appels d'API IAM spécifiques (ListUsers/ListRoles/ListGroups/ListPolicies) et renvoie une liste des politiques et principaux IAM concernés par votre évaluation.

2. Le résultat de l'évaluation des ressources est enregistré et converti en preuves conviviales pour l'auditeur. Audit Manager génère des preuves de données de configuration pour les contrôles qui utilisent des appels d'API en tant que type de source de données. Ces preuves contiennent les données d'origine capturées à partir des réponses de l'API, ainsi que des métadonnées supplémentaires indiquant le contrôle pris en charge par les données.
3. Audit Manager joint les preuves enregistrées au contrôle nommé `MA-5(3) - Citizenship Requirements for Classified Systems` dans votre évaluation.

Comment charger manuellement des preuves pour ce contrôle

Vous pouvez suivre les étapes suivantes pour charger des preuves manuelles à l'appui des preuves automatisées :

1. Placez la documentation relative à la citoyenneté dans un compartiment Amazon Simple Storage Service (Amazon S3) et notez l'URI du S3.
2. Dans votre évaluation Audit Manager, ouvrez le contrôle, accédez à l'onglet des dossiers de preuves et chargez des preuves. Pour ce faire, saisissez l'URI du S3. Pour obtenir des instructions, veuillez consulter la section Ajouter des preuves manuelles dans AWS Audit Manager.
3. Audit Manager joint les preuves chargées au contrôle nommé `MA-5(3) - Citizenship Requirements for Classified Systems` dans votre évaluation.

Comment utiliser Audit Manager pour démontrer la conformité à ce contrôle

Une fois les preuves jointes au contrôle, vous (ou un délégué de votre choix) pouvez les examiner pour déterminer si elles sont suffisantes ou si des mesures correctives sont nécessaires.

Dans cet exemple, vous pouvez examiner les preuves et voir une liste de 20 utilisateurs. Si vous ne savez pas comment identifier les utilisateurs qui font partie du personnel de maintenance, ou si vous ne savez pas quelle est leur nationalité, vous pouvez déléguer ce contrôle à un expert en la matière pour validation. Le délégué peut confirmer la liste du personnel de maintenance et charger manuellement des preuves supplémentaires pour prouver leur statut de citoyenneté. La confirmation de la citoyenneté de tous les utilisateurs concernés de la liste permet de mettre votre environnement AWS en conformité avec les exigences du NIST. Sinon, si votre système ne traite, ne stocke ou ne transmet pas d'informations classifiées, vous pouvez laisser un commentaire expliquant pourquoi ce contrôle n'est pas applicable.

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

Intégrations avec des Services AWS associés

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

AWS Security Hub

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

AWS CloudTrail

AWS CloudTrail vous aide à surveiller les appels passés aux ressources AWS de votre compte. Il s'agit notamment des appels effectués par AWS Management Console, la CLI d'AWS et d'autres Services AWS. Audit Manager collecte les données des journaux directement depuis CloudTrail et convertit les journaux traités en preuves de l'activité utilisateur. Pour plus d'informations sur CloudTrail, consultez Qu'est-ce que AWS CloudTrail ? dans le Guide de l'utilisateur AWS CloudTrail.

AWS Config

AWS Config fournit une vue détaillée de la configuration des ressources AWS de votre Compte AWS. Cela comprend des informations sur la façon dont les ressources sont interreliées et leur configuration passée. Audit Manager capture des instantanés du niveau de sécurité de vos ressources en rapportant les résultats directement depuis AWS Config. Pour plus d'informations sur AWS Config, consultez Qu'est-ce que AWS Config ? dans le guide de l'utilisateur AWS Config.

AWS License Manager

AWS License Manager simplifie le processus d'apport de licences de fournisseurs de logiciels dans le cloud. Lorsque vous construisez une infrastructure cloud sur AWS, vous pouvez économiser en modifiant le rôle de votre inventaire de licence pour une utilisation avec des ressources cloud. Audit Manager fournit un framework de gestion de licences pour vous aider à préparer votre audit.

Ce framework est intégré au gestionnaire de licences pour agréger les informations d'utilisation des licences en fonction des règles de licence définies par le client. Pour plus d'informations sur le gestionnaire de licences, consultez Qu'est-ce que AWS License Manager ? dans le Guide de l'utilisateur AWS License Manager.

AWS Control Tower

AWS Control Tower met en place des barrières de protection préventives et capables de détection pour l'infrastructure cloud. Audit Manager fournit un framework de barrière de protection AWS Control Tower pour vous aider à préparer votre audit. Le framework contient toutes les règles AWS Config basées sur des barrières de protection de AWS Control Tower. Pour plus d'informations sur AWS Control Tower, consultez Qu'est-ce que AWS Control Tower ? dans le guide de l'utilisateur AWS Control Tower.

AWS Artifact

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

Pour obtenir la liste des Services AWS concernés par des programmes de conformité spécifiques, consultez les Services AWS concernés par les programmes de conformité. Pour obtenir plus d'informations générales, consultez Programmes de conformité AWS.

Intégrations avec des produits GRC tiers

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

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

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

Rubriques

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

Comprendre le fonctionnement des intégrations tierces avec Audit Manager

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

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

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

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

sous l'espace de noms AWS Audit Manager de la console Service Quotas. Pour savoir comment demander une augmentation de quota, consultez Gestion de vos quotas d'Audit Manager.

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

Produits partenaires GRC tiers s'intégrant à Audit Manager

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

MetricStream

Pour utiliser cette intégration, contactez MetricStream pour accéder à et acheter le logiciel MetricStream de GRC.

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

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

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

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

Liens MetricStream associés

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

Utiliser d'Audit Manager avec un SDK AWS

Des kits de développement logiciel (SDK) AWS sont disponibles pour de nombreux langages de programmation populaires. Chaque SDK fournit une API, des exemples de code et de la documentation qui peuvent être utilisés par les développeurs pour créer des applications dans leur langage préféré.

Documentation des kits SDK	Documentation spécifique à Audit Manager	Exemples de code	
AWS SDK for C++	Référence d'API AWS SDK for C++ pour Audit Manager	Exemples de code AWS SDK for C++	
AWS SDK for Go	Référence d'API AWS SDK for Go pour Audit Manager	Exemples de code AWS SDK for Go	

Documentation des kits SDK	Documentation spécifique à Audit Manager	Exemples de code
AWS SDK for Java	Référence d'API AWS SDK for Java 2.x pour Audit Manager	Exemples de code AWS SDK for Java
AWS SDK for JavaScript	Référence d'API AWS SDK for JavaScript pour Audit Manager	Exemples de code AWS SDK for JavaScript
AWS SDK for .NET	Référence d'API AWS SDK for .NET pour Audit Manager	Exemples de code AWS SDK for .NET
AWS SDK for PHP	Référence d'API AWS SDK for PHP pour Audit Manager	Exemples de code AWS SDK for PHP
AWS SDK for Python (Boto3)	Référence d'API AWS SDK for Python (Boto) pour Audit Manager	Exemples de code AWS SDK for Python (Boto3)
AWS SDK for Ruby	Référence d'API AWS SDK for Ruby pour Audit Manager	Exemples de code AWS SDK for Ruby

Pour des exemples spécifiques à Audit Manager, veuillez consulter les exemples de code pour AWS Audit Manager.

> **Note**
>
> Audit Manager est disponible dans les versions 1.19.32 et ultérieures de botocore pour le AWS SDK for Python (Boto3). Avant de commencer à utiliser le SDK, assurez-vous que vous utilisez la version appropriée de botocore.

Configuration de AWS Audit Manager

Avant de commencer à utiliser Audit Manager, assurez-vous d'avoir complété les configurations suivantes.

Rubriques

- Prérequis : créez un Compte AWS et configurez des autorisations
- Activer Audit Manager : utilisez la console, le AWS CLI ou l'API pour activer Audit Manager
- Recommandations : configurez les intégrations recommandées avec d'autres Services AWS

Prérequis

Suivez ces étapes pour créer un utilisateur Compte AWS et un utilisateur administratif dotés des privilèges de configuration d'Audit Manager.

Étapes

- S'inscrire à un Compte AWS
- Création d'un utilisateur administratif
- Ajoutez les autorisations requises pour accéder à Audit Manager et l'activer

> **Important**
>
> Si vous êtes déjà configuré avec AWS et IAM, vous pouvez ignorer les étapes 1 et 2. Cependant, vous devez effectuer l'étape 3 pour vous assurer que vous disposez des autorisations requises pour configurer Audit Manager.

S'inscrire à un Compte AWS

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

Pour s'inscrire à un Compte AWS

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

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

Lorsque vous souscrivez à un Compte AWS, un Utilisateur racine d'un compte AWS est créé. Par défaut, seul l'utilisateur root 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 administratif, et à uniquement utiliser l'utilisateur root pour effectuer tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation lorsque le processus d'inscription est terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en cliquant sur Mon compte.

Création d'un utilisateur administratif

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

Sécurisation de votre Utilisateur racine d'un compte AWS

1. Connectez-vous à la AWS Management Console en tant que propriétaire du compte en sélectionnant Root user (Utilisateur racine) et en saisissant l'adresse e-mail de Compte AWS. Sur la page suivante, saisissez votre mot de passe.

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

   Pour obtenir des instructions, consultez Activation d'un dispositif MFA virtuel pour l'utilisateur root de votre Compte AWS (console) dans le Guide de l'utilisateur IAM.

Création d'un utilisateur administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez la section Activer AWS IAM Identity Center du Guide de l'utilisateur AWS IAM Identity Center.

2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur administratif.

   Pour un tutoriel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, consultez la section Configuration de l'accès utilisateur avec le Répertoire IAM Identity Center par défaut du Guide de l'utilisateur AWS IAM Identity Center.

Connexion en tant qu'utilisateur 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 à l'aide d'un utilisateur IAM Identity Center, consultez Connexion au portail d'accès AWS dans le Guide de l'utilisateur Connexion à AWS.

Ajoutez les autorisations requises pour accéder à Audit Manager et l'activer

Vous devez accorder aux utilisateurs les autorisations requises pour activer Audit Manager. Pour les utilisateurs qui ont besoin d'un accès complet à Audit Manager, utilisez la politique gérée AWSAuditManagerAdministratorAccess. Il s'agit d'une politique AWS gérée disponible dans votre Compte AWS et recommandée aux administrateurs d'Audit Manager.

> **Tip**
>
> Comme bonne pratique en matière de sécurité, nous vous recommandons de commencer par les politiques AWS gérées, puis de passer aux autorisations relatives au moindre privilège. Les politiques gérées AWS octroient des autorisations pour de nombreux cas d'utilisation courants. Cependant, gardez à l'esprit qu'étant donné que les stratégies gérées AWS peuvent être utilisées par tous les utilisateurs AWS, elles peuvent ne pas accorder les autorisations de moindre privilège pour vos cas d'utilisation spécifiques. En conséquence, nous vous recommandons de réduire encore les autorisations en définissant des Politiques gérées par le client qui sont spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez la rubrique AWSPolitiques gérées dans le AWS Identity and Access ManagementGuide de l'utilisateur.

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center.

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Pour plus d'informations, voir la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) du Guide de l'utilisateur IAM.

- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM du Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Activer AWS Audit Manager

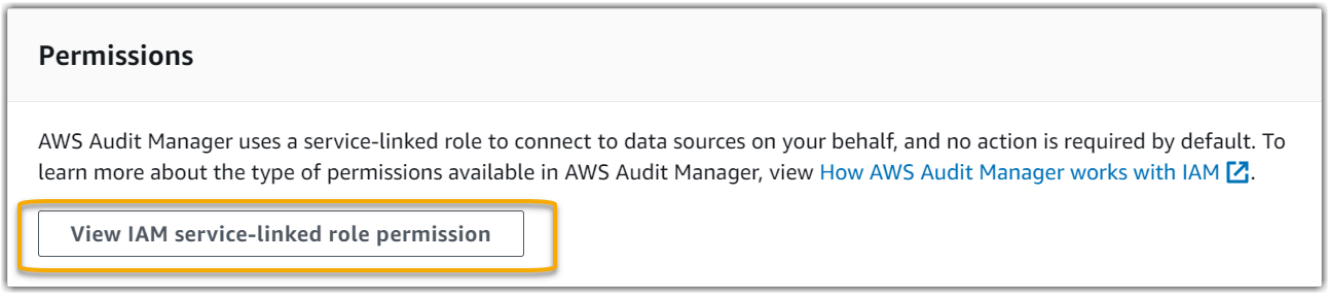
Vous pouvez activer Audit Manager à l'aide de AWS Management Console, l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

Audit Manager console

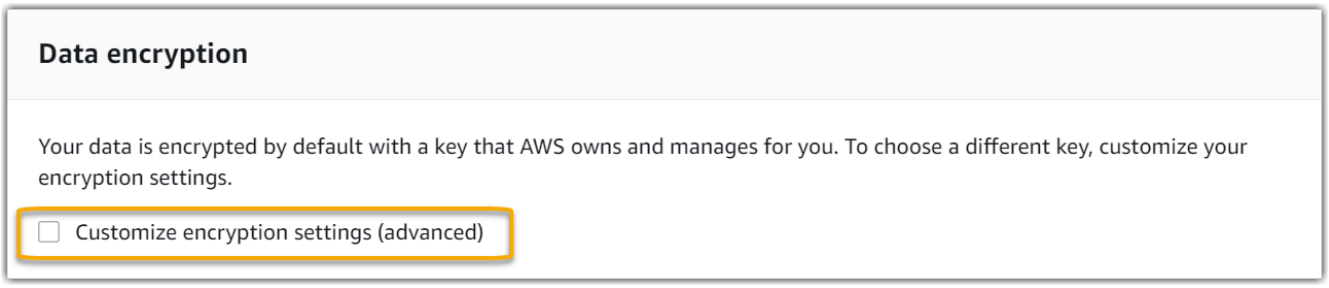
Pour activer Audit Manager à l'aide de la console

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Utilisez les informations d'identification de votre identité IAM pour vous connecter.
3. Choisissez Set up (Configurer)AWS Audit Manager.

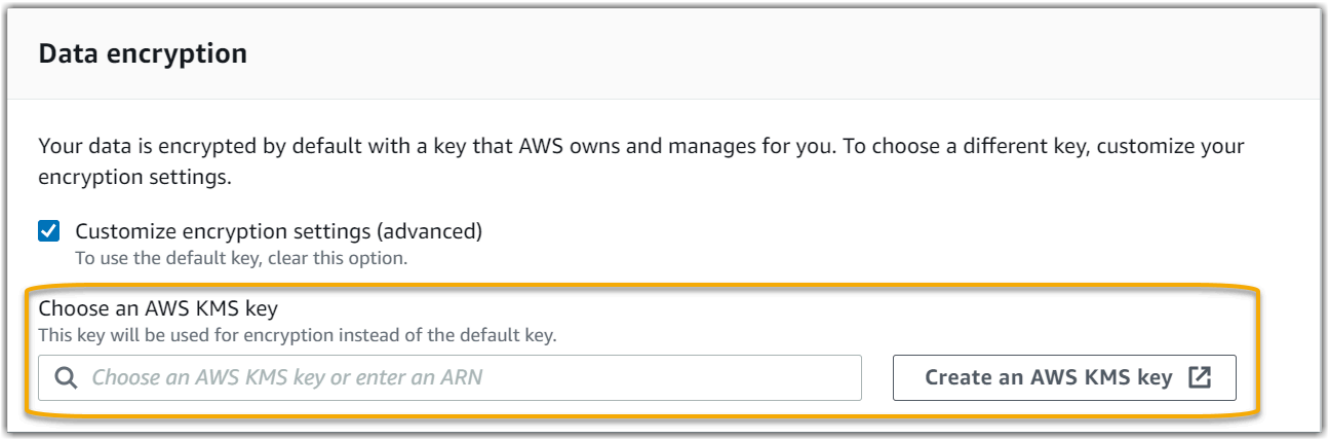
4. Sous Autorisations, aucune action n'est requise. Cela est dû au fait qu'Audit Manager utilise un rôle lié à un service pour se connecter aux sources de données en votre nom. Vous pouvez consulter le rôle lié au service en choisissant Afficher l'autorisation du rôle lié au service IAM.



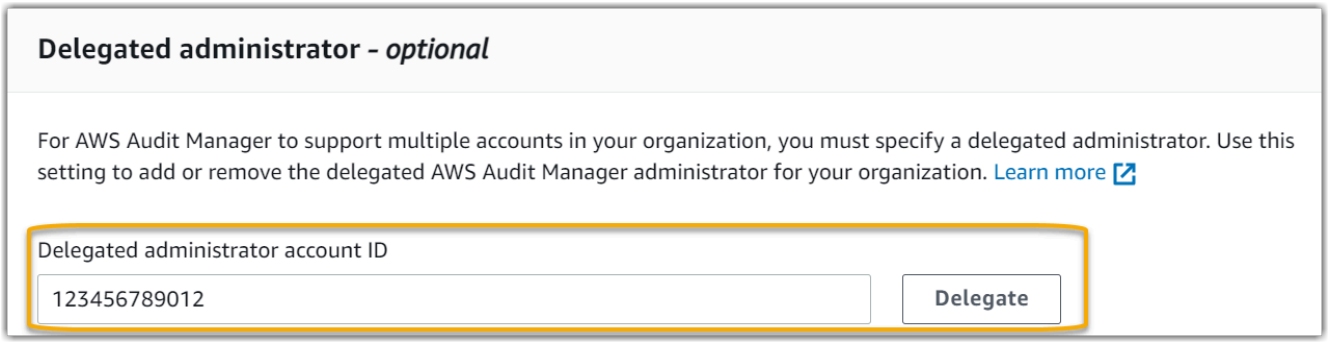
5. Sous Chiffrement des données, l'option par défaut permet à Audit Manager de créer et de gérer un AWS KMS key pour stocker vos données en toute sécurité.



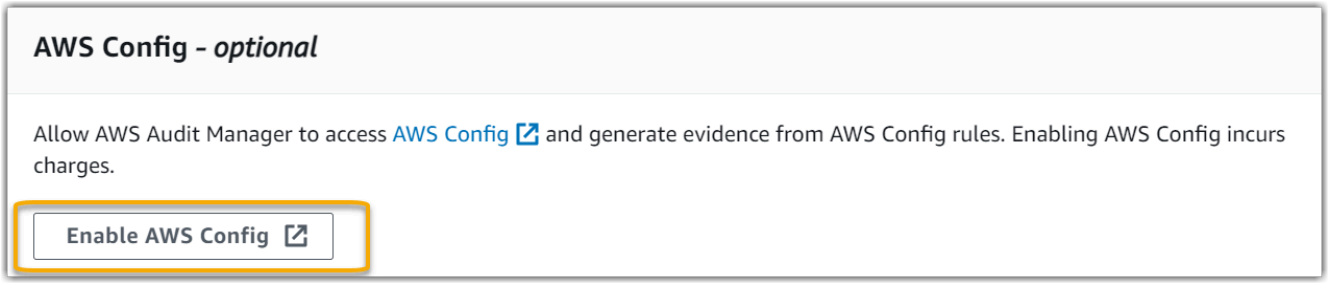
Si vous souhaitez utiliser votre propre clé gérée par le client pour chiffrer les données dans Audit Manager, cochez la case à côté de Personnaliser les paramètres de chiffrement (avancés). Choisissez alors une clé KMS existante ou créez-en une.



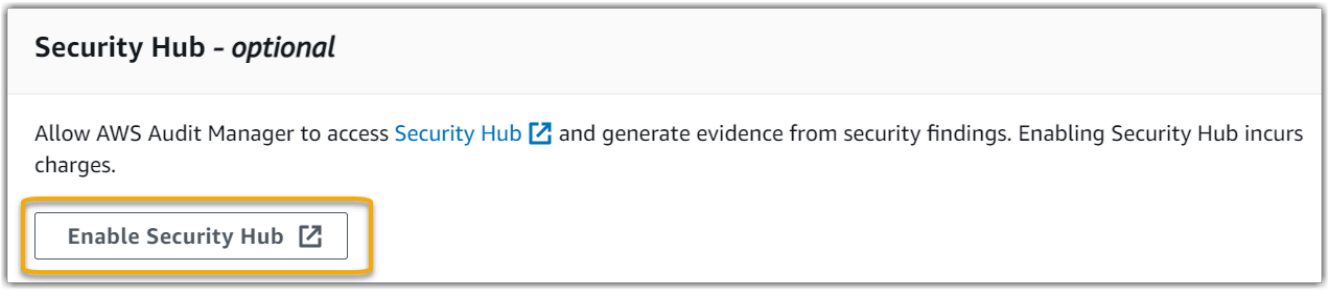
6. (Facultatif) Sous Administrateur délégué : facultatif, vous pouvez spécifier un compte d'administrateur délégué si vous souhaitez qu'Audit Manager exécute des évaluations pour plusieurs comptes. Pour plus d'informations et de recommandations, voir Activer et configurer AWS Organizations pour une utilisation avec Audit Manager.



7. (Facultatif) Sous AWS Config— facultatif, nous vous recommandons d'activer AWS Config pour une expérience optimale. Audit Manager peut alors générer des preuves à l'aide de AWS Config règles. Pour les informations et les options recommandées, voir Activer et configurer AWS Config pour une utilisation avec Audit Manager.



8. (Facultatif) Sous Security Hub – facultatif, nous vous recommandons d'activer Security Hub pour une expérience optimale. Audit Manager peut alors générer des preuves à l'aide des vérification Security Hub. Pour les informations et les options recommandées, voir Activer et configurer AWS Security Hub pour une utilisation avec Audit Manager.



9. Choisissez Compléter la configuration pour terminer le processus de configuration.

AWS CLI

Pour activer Audit Manager à l'aide de AWS CLI

Dans la ligne de commande, exécutez la commande register-account à l'aide des paramètres de configuration suivants :

- `--kms-key` (facultatif) — Utilisez ce paramètre pour chiffrer les données de votre Audit Manager à l'aide de votre propre clé gérée par le client. Si vous ne spécifiez aucune option ici, Audit Manager en crée et gère une AWS KMS key en votre nom pour le stockage sécurisé de vos données.
- `--delegated-admin-account`(facultatif) — Utilisez ce paramètre pour désigner le compte d'administrateur délégué de votre organisation pour Audit Manager. Si vous ne spécifiez aucune option ici, aucun administrateur délégué n'est enregistré.

Exemple d'entrée (remplacez *le texte de l'espace réservé* par vos propres informations) :

```
aws auditmanager register-account \
--kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
--delegated-admin-account 111122224444
```

Exemple de sortie :

```
{
    "status": "ACTIVE"
}
```

Pour plus d'informations sur le AWS CLIet pour obtenir des instructions sur l'installation des outils AWS CLI, consultez les rubriques suivantes dans le AWS Command Line InterfaceGuide de l'utilisateur.

- Guide de l'utilisateur de l'interface de ligne de commande AWS
- Préparation de l'installation de l'AWS Command Line Interface

Audit Manager API

Pour activer Audit Manager à l'aide de l'API Audit Manager

Utilisez l'opération RegisterAccount avec les paramètres de configuration suivants :

- kmsKey (facultatif) - Utilisez ce paramètre pour chiffrer les données de votre Audit Manager à l'aide de votre propre clé gérée par le client. Si vous ne spécifiez aucune option ici, Audit Manager en crée et gère une AWS KMS key en votre nom pour le stockage sécurisé de vos données.
- delegatedAdminAccount (facultatif) - Utilisez ce paramètre pour spécifier le compte d'administrateur délégué de votre organisation pour Audit Manager. Si vous n'en spécifiez aucun, aucun administrateur délégué n'est enregistré.

Exemple d'entrée (remplacez *le texte de l'espace réservé* par vos propres informations) :

```
{
    "kmsKey":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "delegatedAdminAccount":"111122224444"
}
```

Exemple de sortie :

```
{
  "status": "ACTIVE"
}
```

Recommandations

Pour une expérience optimale dans Audit Manager, nous vous recommandons de configurer les fonctionnalités suivantes et d'activer les suivantesServices AWS.

Rubriques

- Configurer les fonctionnalités recommandées d'Audit Manager
- Configurez les intégrations recommandées avec d'autres Services AWS

Configurer les fonctionnalités recommandées d'Audit Manager

Après avoir activé Audit Manager, nous vous recommandons d'activer la fonctionnalité de recherche de preuves.

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

Pour utiliser l'outil de recherche d'éléments probants, vous devez activer cette fonctionnalité dans les paramètres de l'Audit Manager. Pour obtenir des instructions, consultez Paramètres de recherche de preuves.

Configurez les intégrations recommandées avec d'autres Services AWS

Pour une expérience optimale dans Audit Manager, nous vous recommandons vivement d'activer les Services AWS suivants :

- AWS Organizations - Vous pouvez utiliser Organizations pour exécuter des évaluations d'Audit Manager sur plusieurs comptes et consolider les preuves dans un compte d'administrateur délégué.
- AWS Security Hubet AWS Config— Lorsque vous activez Services AWS, ils peuvent être utilisés comme type de source de données pour les contrôles dans le cadre de vos évaluations d'Audit Manager. Audit Manager peut ensuite communiquer les résultats des contrôles de conformité directement depuis ces services.

Rubriques

- Activer et configurer AWS Config (facultatif)

- Activer et configurer AWS Security Hub (facultatif)
- Activer AWS Organizations (facultatif)

Activer et configurer AWS Config (facultatif)

Dans Audit Manager, de nombreux contrôles sont utilisés AWS Config comme type de source de données. Pour prendre en charge ces contrôles, vous devez les activer AWS Config sur tous les comptes sur chaque Région AWS où Audit Manager est activé. Si Audit Manager essaie de collecter des preuves pour les contrôles utilisant AWS Config comme type de source de données et que les AWS Config règles associées ne sont pas activées, aucune preuve n'est collectée pour ces contrôles.

Audit Manager ne se débrouille pas AWS Config à votre place. Vous pouvez suivre ces étapes pour activer AWS Config et configurer ses paramètres.

Tâches à intégrer AWS Config à Audit Manager

- Étape 1 : Activer AWS Config
- Étape 2 : configurer vos AWS Config paramètres pour une utilisation avec Audit Manager

Étape 1 : Activer AWS Config

Vous pouvez activer AWS Config à l'aide de la console AWS Config ou de l'API. Pour obtenir des instructions, consultez la section Mise en route avec AWS Config dans le AWS Config Guide du développeur.

Étape 2 : configurer vos AWS Config paramètres pour une utilisation avec Audit Manager

> **Important**
>
> L'activation de AWS Config est une recommandation facultative. Toutefois, si vous activez AWS Config, les paramètres suivants sont obligatoires.

Après l'activationAWS Config, assurez-vous d'activer également AWS Config les règles ou de déployer un pack de conformité pour la norme de conformité associée à votre audit. Cette étape permet à Audit Manager d'importer les résultats des règles AWS Config que vous avez activées.

Après avoir activé une règle AWS Config, nous vous recommandons de passer en revue les paramètres de cette règle. Vous devez ensuite valider ces paramètres par rapport aux exigences du framework de conformité que vous avez choisi. Si nécessaire, vous pouvez mettre à jour les paramètres d'une règle AWS Config pour vous assurer qu'elle est conforme aux exigences du framework. Vous pouvez ainsi garantir que vos évaluations collectent les preuves de contrôle de conformité correctes pour un framework donné.

Supposons, par exemple, que vous créez une évaluation pour CIS v1.2.0. Ce framework comporte un contrôle nommé 1.4 — Assurez-vous que les clés d'accès sont renouvelées tous les 90 jours ou moins. DansAWS Config, la règle de rotation des clés d'accès comporte un `maxAccessKeyAge` paramètre dont la valeur par défaut est de 90 jours. Par conséquent, la règle s'aligne sur les exigences de contrôle. Si vous n'utilisez pas la valeur par défaut, assurez-vous qu'elle est égale ou supérieure à l'exigence de 90 jours de CIS v1.2.0.

Vous trouverez les détails des paramètres par défaut pour chaque règle gérée dans la documentation AWS Config. Pour obtenir des instructions sur la façon de configuration d'une règle, consultez la section Utilisation des règles AWS Config gérées.

Activer et configurer AWS Security Hub (facultatif)

Dans Audit Manager, de nombreux contrôles utilisent Security Hub comme type de source de données. Pour prendre en charge ces contrôles, vous devez les activer Security Hub sur tous les comptes sur chaque région où Audit Manager est activé. Si Audit Manager essaie de collecter des preuves pour les contrôles utilisant Security Hub comme type de source de données et que les règles Security Hub associées ne sont pas activées, aucune preuve n'est collectée pour ces contrôles.

Audit Manager ne gère pas Security Hub à votre place. Vous pouvez suivre ces étapes pour activer Security Hub et configurer ses paramètres.

Tâches à intégrer AWS Security Hub à Audit Manager

- Étape 1 : Activer AWS Security Hub
- Étape 2 : configurer vos paramètres Security Hub pour une utilisation avec Audit Manager

Étape 1 : Activer AWS Security Hub

Vous pouvez activer Security Hub à l'aide de la console ou de l'API. Pour obtenir des instructions, consultez ConfigurationAWS Security Hub dans le guide de l'utilisateur AWS Security Hub.

Étape 2 : configurer vos paramètres Security Hub pour une utilisation avec Audit Manager

> **Important**
>
> L'activation de Security Hub est une recommandation facultative. Toutefois, si vous activez Security Hub, les paramètres suivants sont obligatoires.

Après avoir activé Security Hub, assurez-vous d'effectuer également les opérations suivantes :

- Activer AWS Config et configurer l'enregistrement des ressources : Security Hub utilise des règles AWS Config liées aux services pour effectuer la plupart de ses contrôles de sécurité. Pour prendre en charge ces contrôles, AWS Config doivent être activés et configurés pour enregistrer les ressources requises pour les contrôles que vous avez activés dans chaque norme activée.
- Activer toutes les normes de sécurité : cette étape permet à Audit Manager d'importer les résultats correspondant à toutes les normes de conformité prises en charge.
- Activez le paramètre des résultats de contrôle consolidés dans Security Hub.- Ce paramètre est activé par défaut si vous activez Security Hub le 23 février 2023 ou après cette date.

> **Note**
>
> Lorsque vous activez les résultats consolidés, Security Hub produit un résultat unique pour chaque contrôle de sécurité (même lorsque le même contrôle est utilisé pour plusieurs normes). Chaque résultat du Security Hub est collecté dans le cadre d'une évaluation de ressource unique dans Audit Manager. Par conséquent, les résultats consolidés se traduisent par une diminution du nombre total d'évaluations uniques des ressources effectuées par Audit Manager pour les résultats de Security Hub. Pour cette raison, l'utilisation de résultats consolidés peut souvent entraîner une réduction des coûts d'utilisation de votre Audit Manager. Pour plus d'informations sur l'utilisation de Security Hub comme type de source de données, consultez AWS Security Hub commandes prises en charge par AWS Audit Manager. Pour plus d'informations sur la tarification d'Audit Manager, consultez AWS Audit Manager Tarification.

Si vous utilisez AWS Organizations et souhaitez collecter des preuves Security Hub à partir de vos comptes membres, vous devez également suivre les étapes suivantes dans Security Hub.

Pour configurer les paramètres Security Hub de votre organisation

1. Connectez-vous à la AWS Management Console et ouvrez la console AWS Security Hub à l'adresse https://console.aws.amazon.com/securityhub/.
2. À l'aide de votre compte de gestion AWS Organizations, désignez un compte en tant qu'administrateur délégué pour Security Hub. Pour plus d'informations, consultez Désignation d'un compte administrateur Security Hub dans le Guide de l'utilisateur AWS Security Hub.

   > **Note**
   >
   > Vérifiez que le compte d'administrateur délégué que vous utilisez dans Security Hub est le même que celui que vous utilisez dans Audit Manager.

3. À l'aide de votre compte d'administrateur délégué d'organisations, allez dans Paramètres, Comptes, sélectionnez tous les comptes, puis ajoutez-les en tant que membres en sélectionnant Inscription automatique. Pour plus d'informations, consultez la rubrique Activation de comptes membre de votre organisation du Guide de l'utilisateur AWS Security Hub.
4. Activez AWS Config pour chaque compte membre de l'organisation. Pour plus d'informations, consultez la rubrique Activation de comptes membre de votre organisation du Guide de l'utilisateur AWS Security Hub.
5. Activez la norme de sécurité PCI DSS pour chaque compte membre de l'organisation. La norme AWS CIS Foundations Benchmark et la norme AWS Foundational Best Practices sont déjà activées par défaut. Pour plus d'informations, consultez la rubrique Activation d'une norme de sécurité dans le AWS Security HubGuide de l'utilisateur.

Activer AWS Organizations (facultatif)

Audit Manager prend en charge plusieurs comptes via l'intégration avec AWS Organizations. Audit Manager peur exécuter des évaluations sur plusieurs comptes et consolider les preuves dans un compte d'administrateur délégué. L'administrateur délégué dispose des autorisations nécessaires pour créer et gérer des ressources Audit Manager avec l'organisation comme zone de confiance. Seul le compte de gestion peut désigner un administrateur délégué.

Tâches à intégrer AWS Organizations à Audit Manager

- Étape 1 : créer une organisation ou y adhérer
- Étape 2 : activer toutes les fonctionnalités de votre organisation

- Étape 3 : spécifier un administrateur délégué pour Audit Manager

Étape 1 : créer une organisation ou y adhérer

Si votre Compte AWS ne fait pas partie d'une organisation, vous pouvez créer ou rejoindre une organisation. Pour obtenir des instructions pratiques, veuillez consulter Création et gestion d'une organisation dans le Guide de l'utilisateur AWS Organizations.

Étape 2 : activer toutes les fonctionnalités de votre organisation

Vous devez ensuite activer toutes les fonctionnalités de votre organisation. Pour obtenir les instructions, consultez Activation de toutes les fonctionnalités de votre organisation dans le Guide de l'utilisateur AWS Organizations.

Étape 3 : spécifier un administrateur délégué pour Audit Manager

Nous vous recommandons d'activer Audit Manager à l'aide d'un compte de gestion des organisations puis de spécifier un administrateur délégué. Ensuite, vous pouvez utiliser le compte d'administrateur délégué pour vous connecter et exécuter des évaluations. À titre de bonne pratique, nous vous recommandons de créer uniquement des évaluations à l'aide du compte administrateur délégué plutôt que du compte de gestion.

> **Warning**
>
> Une fois que vous avez désigné un administrateur délégué à l'aide d'un compte de gestion des organisations, celui-ci ne peut plus créer d'évaluations supplémentaires dans Audit Manager. En outre, la collecte de preuves s'arrête pour toutes les évaluations existantes créées par le compte de gestion. Au lieu de cela, Audit Manager collecte et joint des preuves à l'administrateur délégué, qui est le principal responsable de la gestion des évaluations de votre organisation.

Pour ajouter ou modifier un administrateur délégué après avoir activé Audit Manager, consultez AWS Audit Managerparamètres, Administrateur délégué.

Points à prendre en compte :

- Vous ne pouvez pas utiliser votre compte de gestion en tant qu'administrateur délégué dans Audit Manager.

- Si vous souhaitez activer Audit Manager dans plusieurs Région AWS, vous devez désigner un compte d'administrateur délégué séparément dans chaque région. Dans les paramètres de votre Audit Manager, vous devez désigner le même compte d'administrateur délégué dans toutes les régions.
- Si vous avez fourni une clé gérée par le client lorsque vous avez activé Audit Manager, assurez-vous que le compte d'administrateur délégué a accès à cette clé KMS. Pour consulter et modifier les paramètres de chiffrement de l'Audit Manager, consultez Chiffrement des données.
- Pour des solutions aux problèmes courants liés aux Organisations et aux administrateurs délégués dans Audit Manager, consultez Résolution des problèmes liés aux administrateurs délégués et à AWS Organizations.

Que puis-je faire ensuite ?

Maintenant que vous avez configuré Audit Manager, vous êtes prêt à commencer à utiliser le service. Vous pouvez également accéder à la page des paramètres de la console pour mettre à jour les paramètres que vous avez choisis lors de la configuration d'Audit Manager.

Démarrer avec Audit Manager

Vous pouvez démarrer dans Audit Manager en suivant un didacticiel qui explique comment créer votre première évaluation. Pour plus d'informations, voir Tutoriel pour les responsables d'audit : création d'une évaluation.

Mettez à jour vos paramètres d'Audit Manager

Vous pouvez mettre à jour vos paramètres à tout moment. Pour de plus amples informations, veuillez consulter Paramètres AWS Audit Manager.

Démarrer avec AWS Audit Manager

Utilisez les tutoriels étape par étape de cette section pour apprendre à utiliser AWS Audit Manager.

Tip

Les tutoriels suivants sont classés par public. Choisissez le tutoriel qui vous convient en fonction de votre rôle en tant que responsable de l'audit ou délégué.

- Les responsables de l'audit sont des utilisateurs d'Audit Manager chargés de créer et de gérer les évaluations. Dans le monde des affaires, les responsables de l'audit sont généralement des professionnels de la gouvernance, de la gestion des risques et de la conformité (GRC). Dans le contexte d'Audit Manager, toutefois, les membres des équipes SecOps ou DevOps peuvent également assumer la personnalité d'un responsable de l'audit. Les responsables de l'audit peuvent demander l'assistance d'un expert en la matière, également appelé délégué, pour vérifier des contrôles spécifiques et valider les preuves. Les responsables de l'audit doivent posséder les autorisations nécessaires pour gérer une évaluation.
- Les délégués sont des experts en la matière dotés d'une expertise technique ou commerciale spécialisée. Bien qu'ils ne possèdent ni ne gèrent les évaluations d'Audit Manager, ils peuvent tout de même y contribuer. Les délégués aident les responsables de l'audit dans des tâches telles que la validation des preuves relatives aux contrôles relevant de leur domaine d'expertise. Les délégués disposent d'autorisations limitées dans Audit Manager. La raison en est que les responsables de l'audit délèguent des ensembles de contrôles spécifiques pour vérification, et non des évaluations complètes.

Pour plus d'informations sur ces personas et les autres concepts d'Audit Manager, consultez la section Propriétaires de l'audit et Délégués dans la Concepts et terminologie AWS Audit Manager section de ce guide. Pour plus d'informations sur les autorisations IAM recommandées pour chaque persona, consultez Politiques recommandées pour les personas utilisateurs dans AWS Audit Manager.

Tutoriels Audit Manager

Création d'une évaluation

Public cible : Responsables de l'audit

Vue d'ensemble : Suivez les instructions étape par étape pour créer votre première évaluation et être rapidement opérationnel. Ce tutoriel vous explique comment utiliser un framework standard pour créer une évaluation et commencer la collecte automatisée de preuves.

Vérification d'un ensemble de contrôles

Public : Délégués

Vue d'ensemble : aidez le responsable de l'audit en vérifiant les preuves relatives aux contrôles relevant de votre domaine d'expertise. Découvrez comment vérifier les ensembles de contrôles et les preuves associées, ajouter des commentaires, charger des preuves supplémentaires et mettre à jour le statut de chacun des contrôles.

Tutoriel pour les responsables d'audit : création d'une évaluation

Ce tutoriel présente une introduction à AWS Audit Manager. Dans ce tutoriel, vous allez créer une évaluation à l'aide de AWS Audit Manager Sample Framework. En créant une évaluation, vous lancez le processus continu de collecte automatisée de preuves pour les contrôles dans ce framework.

Ce tutoriel montre comment :

- Sélectionner un framework standard sur lequel créer une évaluation
- Préciser les AWS comptes à inclure dans votre évaluation
- Préciser les AWS services à inclure dans votre évaluation
- Préciser les responsables de l'audit pour votre évaluation
- Vérifier et créer votre évaluation

Avant de commencer ce tutoriel, vérifiez d'abord que vous remplissez les conditions suivantes :

- Vous avez rempli tous les prérequis décrits dans Configuration de AWS Audit Manager. Vous devez utiliser votre compte AWS et la console AWS Audit Manager pour suivre ce tutoriel.

- Votre identité IAM est dotée des autorisations appropriées pour créer et gérer une évaluation dans AWS Audit Manager. Les deux politiques suggérées qui accordent ces autorisations sont l'exemple 2 : autoriser l'accès complet à l'administrateur et l'exemple 3 : autoriser l'accès à la gestion.
- Vous connaissez la terminologie et les fonctionnalités d'Audit Manager. Pour une présentation générale, consultez Qu'est-ce qu'AWS Audit Manager ? et Concepts et terminologie AWS Audit Manager.

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

Étape 1 : Indiquer les détails de l'évaluation

Pour la première étape, sélectionnez un framework et fournissez des informations de base pour votre évaluation.

Pour indiquer les détails de l'évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Choisissez LaunchAWS Audit Manager.
3. Dans le volet de navigation, choisissez Mise en route, puis Démarrer avec un framework.
4. Choisissez le framework de votre choix, puis choisissez Créer une évaluation à partir du framework. Cet exemple utilise le modèle AWS Audit Manager Sample Framework.
5. Sous Nom de l'évaluation, saisissez un nom pour votre évaluation.
6. (Facultatif) Sous Description de l'évaluation, saisissez une description pour votre évaluation.
7. Sous Destination des rapports d'évaluation, choisissez le compartiment Amazon S3 dans lequel vous souhaitez enregistrer vos rapports d'évaluation.

8. Sous Frameworks, vérifiez que AWS Audit ManagerSample Framework (ou le framework de votre choix) est sélectionné.
9. Sous Balises, choisissez Ajouter une nouvelle balise pour associer une balise à votre évaluation. Vous pouvez indiquer une clé et une valeur pour chaque balise. La clé de balise est obligatoire et peut être utilisée comme critère de recherche lorsque vous recherchez cette évaluation. Pour plus d'informations sur les balises dans AWS Audit Manager, consultez Balisage de ressources AWS Audit Manager.
10. Choisissez Suivant.

Étape 2 : Indiquer les comptes AWS concernés

Ensuite, indiquez les comptes AWS que vous souhaitez inclure dans le champ de votre évaluation.

AWS Audit Manager s'intègre à AWS Organizations, ainsi vous pouvez exécuter une évaluation Audit Manager sur plusieurs comptes et consolider les preuves dans un compte d'administrateur délégué. Pour activer Organizations dans Audit Manager (si ce n'est pas déjà fait), consultez Activer AWS Organizations (facultatif) sur la page Configuration de ce guide.

> **Note**
>
> Audit Manager peut prendre en charge jusqu'à 150 comptes dans le cadre d'une évaluation. Si vous essayez d'inclure plus de 150 comptes, la création de l'évaluation risque d'échouer.

Pour indiquer les comptes concernés

1. Sous AWScomptes, sélectionnez les comptes AWS que vous souhaitez inclure dans le champ de votre évaluation.
   - Si vous avez activé Organizations dans AWS Audit Manager, plusieurs comptes sont répertoriés.
   - Si vous n'avez pas activé Organizations dans Audit Manager, seul votre compte actuel est répertorié.
2. Choisissez Suivant.

Étape 3 : Indiquer des services AWS concernés

Le cadre que vous avez sélectionné précédemment définit les services AWS qu'Audit Manager surveille et pour lesquels il collecte des preuves.

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir d'un framework standard, la liste des services concernés est présélectionnée et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework standard. Si un service AWS répertorié n'est pas sélectionné, Audit Manager ne collecte pas de preuves auprès des ressources liées à ce service. C'est également le cas s'il est sélectionné mais que vous ne l'avez pas inscrit dans votre environnement.

À cette étape du tutoriel, vous pouvez vérifier les services AWS concernés par l'évaluation en fonction de la définition du framework. Pour en savoir plus sur les frameworks et sur la façon d'y accéder et de les vérifier, consultez la section Bibliothèque de frameworks de ce guide.

Pour indiquer les services AWS concernés

1. Dans la section AWSServices, consultez la liste des services concernés par cette évaluation.
2. Choisissez Suivant.

> **Tip**
>
> Si vous devez modifier la liste des services concernés, vous pouvez le faire en utilisant l'API CreateAssessment fournie par Audit Manager.
> Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Étape 4 : Indiquer les responsables de l'audit

Dans cette étape, vous indiquez les responsables de l'audit pour votre évaluation. Les responsables de l'audit sont les personnes de votre lieu de travail, généralement issues des équipes GRC, SecOps ou DevOps, qui sont chargées de gérer l'évaluation de l'Audit Manager. Nous leur recommandons d'utiliser la politique d'accès AWSAuditManagerAdministratorAccess.

Pour indiquer les responsables de l'audit

1. Sous Responsables de l'audit, choisissez les responsables de l'audit pour votre évaluation. Pour trouver d'autres responsables d'audit, utilisez la barre de recherche pour effectuer une recherche par nom ou par compte AWS.
2. Choisissez Suivant.

Étape 5 : Vérification et création

Vérifiez les informations de votre évaluation. Pour modifier les informations d'une étape, choisissez Modifier. Lorsque vous avez terminé, choisissez Créer une évaluation pour lancer votre première évaluation et commencer la collecte continue de preuves.

Une fois que vous avez créé une évaluation, la collecte de preuves se poursuit jusqu'à ce que vous passiez le statut de l'évaluation à inactif. Vous pouvez également arrêter la collecte de preuves pour un contrôle précis en faisant passer le statut du contrôle à inactif.

> **Note**
>
> Les preuves automatisées sont disponibles 24 heures après la création de l'évaluation. AWS Audit Manager collecte automatiquement des preuves à partir de plusieurs sources de données, et la fréquence de cette collecte de preuves est basée sur le type de preuves. Pour plus d'informations, consultez Fréquence de collecte des preuves dans ce guide.

Comment procéder ensuite ?

Nous vous recommandons de continuer à vous renseigner sur les concepts et les outils présentés dans ce didacticiel. Pour ce faire, consultez les ressources suivantes :

- Vérification d'une évaluation — Vous présente la page d'évaluation où vous pouvez explorer les différents éléments de votre évaluation.
- Évaluations dans AWS Audit Manager — S'appuie sur ce tutoriel et fournit des informations approfondies sur les concepts et les tâches de gestion d'une évaluation. Dans ce document, nous vous recommandons particulièrement de consulter les rubriques suivantes :
  - Comment créer une évaluation à partir d'un autre framework

  - Comment vérifier les preuves d'une évaluation et générer un rapport d'évaluation
  - Comment modifier le statut d'une évaluation ou supprimer une évaluation
- Bibliothèque de frameworks — Présente la bibliothèque de cadres et explique comment créer un framework personnalisé pour vos propres besoins de conformité spécifiques.
- Bibliothèque de contrôles—Présente la bibliothèque de contrôles et explique comment créer un contrôle personnalisé à utiliser dans votre framework personnalisé.
- Concepts et terminologie AWS Audit Manager — Fournit les définitions des concepts et de la terminologie utilisés dans Audit Manager.
- [Vidéo] Collectez des preuves et gérez les données d'audit à l'aide de AWS Audit Manager : montre le processus de création d'une évaluation décrit dans ce tutoriel, ainsi que d'autres tâches telles que la vérification d'un contrôle et la génération d'un rapport d'évaluation.

Tutoriel pour les délégués : Vérification d'un ensemble de contrôles

Ce tutoriel explique comment vérifier un ensemble de contrôles qui a été partagé avec vous par un responsable d'audit dans AWS Audit Manager.

Les responsables de l'audit utilisent Audit Manager pour créer des évaluations et collecter des preuves pour les contrôles répertoriés dans cette évaluation. Les responsables d'audit peuvent parfois avoir des questions ou besoin d'aide pour valider les éléments probants d'une série de contrôles. Dans ce cas, le responsable de l'audit peut déléguer un ensemble de contrôles à un expert en la matière pour vérification.

En tant que délégué, vous aidez les responsables de l'audit à vérifier les preuves collectées pour les contrôles relevant de votre domaine d'expertise.

Ce tutoriel montre comment :

- Accéder aux notifications qui vous ont été envoyées par le responsable de l'audit
- Vérifier un ensemble de contrôles et les éléments de preuve connexes
- Télécharger des preuves manuelles à l'appui d'un contrôle
- Ajouter un commentaire pour un contrôle que vous êtes en train de vérifier
- Mettre à jour le statut d'un contrôle
- Soumettre l'ensemble de contrôles révisé au responsable de l'audit lorsque votre vérification est terminée

Avant de commencer ce tutoriel, vérifiez d'abord que vous remplissez les conditions suivantes :

- Votre compte AWS est configuré. Pour terminer ce tutoriel, vous devez utiliser à la fois votre compte AWS et la console AWS Audit Manager. Pour de plus amples informations, veuillez consulter Configuration de AWS Audit Manager.
- Vous connaissez la terminologie et les fonctionnalités d'Audit Manager. Pour une présentation générale d'Audit Manager, reportez-vous aux sections Qu'est-ce qu'AWS Audit Manager ? et Concepts et terminologie AWS Audit Manager.

Étape 1 : Accéder à vos notifications

Commencez par vous connecter à AWS Audit Manager, où vous pouvez accéder à vos notifications pour voir les ensembles de contrôle qui vous ont été délégués pour vérification.

Pour accéder à vos notifications

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation de gauche, choisissez Notifications. Ou, dans la barre d'éclair bleue en haut de la page, choisissez Afficher la notification pour ouvrir la page des notifications.
3. Sur la page Notifications, vous pouvez consulter la liste des ensembles de contrôles qui vous ont été délégués. Les tableaux de notifications comprennent les informations suivantes :
   - Date : date à laquelle l'ensemble de contrôles a été délégué.
   - Évaluation : nom de l'évaluation associée à l'ensemble de contrôles. Vous pouvez choisir un nom d'évaluation pour ouvrir la page détaillée de l'évaluation.
   - Ensemble de contrôles : nom du jeu de contrôles qui vous a été délégué pour vérification.
   - Source : utilisateur ou rôle qui vous a délégué l'ensemble de contrôle.
   - Description : les instructions de vérification fournies par le responsable de l'audit.

> **Tip**
>
> Vous pouvez également vous abonner à une rubrique SNS pour recevoir des alertes par e-mail lorsqu'un ensemble de contrôles vous est attribué pour vérification. Pour de plus amples informations, veuillez consulter Notifications dans AWS Audit Manager.

Étape 2 : Vérifier l'ensemble de contrôles et les éléments de preuve connexes

L'étape suivante consiste à vérifier les ensembles de contrôles que le responsable de l'audit vous a délégués. En examinant les contrôles et leurs preuves, vous pouvez déterminer si une action supplémentaire est nécessaire pour un contrôle. Les actions supplémentaires peuvent inclure le téléchargement manuel de preuves supplémentaires pour démontrer la conformité ou le dépôt d'un commentaire sur ce contrôle.

Pour vérifier un ensemble de contrôles

1. À partir de la page Notifications, vérifiez la liste des ensembles de contrôles qui vous ont été délégués. Identifiez ensuite celui que vous souhaitez vérifier et choisissez le nom de l'évaluation correspondante.
2. Sous l'onglet Contrôles de la page détaillée de l'évaluation, faites défiler la page vers le bas jusqu'au tableau Séries de contrôles.
3. Dans la colonne Contrôles regroupés par séries de contrôles, cliquez sur le nom d'une série de contrôles pour en afficher le détail. Puis, sélectionnez le nom d'un contrôle pour ouvrir sa page détaillée.
4. (Facultatif) Choisissez Mettre à jour le statut du contrôle pour modifier le statut du contrôle. Pendant que votre vérification est en cours, vous pouvez marquer le statut comme En cours de vérification.
5. Consultez les informations relatives au contrôle dans les onglets Dossiers d'éléments probants, Sources de données, Commentaires et Journal des modifications. Pour plus d'informations sur chacun de ces onglets et sur la façon d'interpréter les données qu'ils contiennent, consultez la section Vérification des contrôles dans une évaluation.

Pour vérifier les éléments probants d'un contrôle

1. Sur la page détaillée du contrôle, choisissez l'onglet Dossiers d'éléments probants.
2. Accédez au tableau Dossiers de preuves, où la liste des dossiers contenant les preuves de ce contrôle est affichée. Ces dossiers sont organisés et nommés en fonction de la date à laquelle les preuves contenues dans ce dossier ont été collectées.
3. Sélectionnez le nom d'un dossier d'éléments probants pour l'ouvrir. À partir de là, vous pouvez consulter un résumé de toutes les preuves recueillies à cette date. Ce résumé inclut également

le nombre total de problèmes de contrôle de conformité signalés directement par AWS Security Hub, AWS Config ou par les deux. Pour obtenir des instructions sur la façon d'interpréter les données de cette page, consultez Vérification des dossiers d'éléments probants.

4. À partir de la page récapitulative du dossier de preuves, accédez au tableau éléments probants. Dans la colonne Heure, choisissez une rubrique pour ouvrir et vérifier les détails des preuves recueillies à ce moment-là. Pour obtenir des instructions sur la façon d'interpréter les données de cette page, consulter Vérification d'une preuve individuelle.

Étape 3. Charger des preuves manuelles (facultatif)

Bien que AWS Audit Manager collecte automatiquement des preuves pour de nombreux contrôles, dans certains cas, vous devrez peut-être fournir des preuves supplémentaires. Dans ces cas, vous pouvez télécharger manuellement des preuves qui vous aident à démontrer le respect de ce contrôle.

Avant de pouvoir télécharger des preuves manuelles dans votre évaluation, vous devez d'abord les placer dans un compartiment S3. Pour des instructions, consultez les rubriques Création d'un compartiment et Chargement d'objets dans le Guide de l'utilisateur d'Amazon Simple Storage Service.

> **Important**
>
> Chaque compte AWS ne peut télécharger manuellement que 100 fichiers de preuves maximum pour un contrôle par jour. Le dépassement de ce quota quotidien entraîne l'échec de tout chargement manuel supplémentaire pour le contrôle en question. Si vous devez charger une grande quantité de preuves manuelles dans un seul contrôle, chargez-les par lots sur plusieurs jours.

Pour charger des preuves manuelles à l'appui d'un contrôle

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. À partir de la page Notifications, vous pouvez consulter la liste des ensembles de contrôles qui vous ont été délégués. Identifiez l'ensemble de contrôles pour lequel vous souhaitez ajouter des preuves et choisissez le nom de l'évaluation associée pour ouvrir la page détaillée de l'évaluation.

3. Choisissez l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'à Ensembles de contrôles, puis sélectionnez le nom d'un contrôle pour l'ouvrir.
4. Choisissez l'onglet Dossiers de preuves, puis choisissez Charger des preuves manuelles.
5. Sur la page suivante, saisissez l'URI S3 des preuves. Vous pouvez trouver l'URI S3 en accédant à l'objet dans la console Amazon S3 et en choisissant Copy S3 URI.
6. Choisissez Charger pour charger les preuves manuelles.

> **Note**
>
> Lorsqu'un contrôle est inactif, vous ne pouvez pas charger de preuves manuelles pour ce contrôle. Pour charger des preuves manuelles dans un contrôle, vous devez d'abord faire passer le statut du contrôle sur en cours de vérification ou vérifié. Pour obtenir des instructions sur la façon de modifier le statut d'un contrôle, reportez-vous à la section Étape 5 : Marquer un contrôle comme vérifié (facultatif).

Étape 4. Ajouter un commentaire pour un contrôle (facultatif)

Vous pouvez ajouter des commentaires pour tous les contrôles que vous vérifiez. Ces commentaires sont visibles par le responsable de l'audit. Par exemple, vous pouvez laisser un commentaire pour fournir une mise à jour du statut et confirmer que vous avez résolu tout problème lié à ce contrôle.

Pour ajouter un commentaire à un contrôle

1. À partir de la page Notifications, vérifiez la liste des ensembles de contrôles qui vous ont été délégués. Recherchez l'ensemble de contrôles pour lequel vous souhaitez laisser un commentaire, puis choisissez le nom de l'évaluation associée.
2. Choisissez l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'à Ensembles de contrôles, puis sélectionnez le nom d'un contrôle pour l'ouvrir.
3. Sélectionnez l'onglet Commentaires.
4. Sous Envoyer des commentaires, saisissez votre commentaire dans la zone de texte.
5. Choisissez Soumettre un commentaire pour ajouter votre commentaire. Votre commentaire apparaît désormais dans la section Commentaires précédents de la page, avec tout autre commentaire concernant ce contrôle.

Étape 5 : Marquer un contrôle comme vérifié (facultatif)

La modification du statut d'un contrôle est facultative. Cependant, nous vous recommandons de modifier le statut de chaque contrôle sur Vérifié au fur et à mesure de votre vérification de ce contrôle. Quel que soit le statut de chaque contrôle individuel, vous pouvez toujours soumettre les contrôles au responsable de l'audit.

Pour marquer un contrôle comme vérifié

1. À partir de la page Notifications, vérifiez la liste des ensembles de contrôles qui vous ont été délégués. Recherchez le jeu de contrôles qui contient le contrôle que vous souhaitez marquer comme vérifié. Choisissez ensuite le nom de l'évaluation associée pour ouvrir la page détaillée de l'évaluation.
2. Sous l'onglet Contrôles de la page détaillée de l'évaluation, faites défiler la page vers le bas jusqu'au tableau Séries de contrôles.
3. Dans la colonne Contrôles regroupés par séries de contrôles, cliquez sur le nom d'une série de contrôles pour en afficher le détail. Choisissez le nom d'un contrôle pour ouvrir la page détaillée du contrôle.
4. Choisissez Mettre à jour le statut du contrôle et remplacez le statut par Vérifié.
5. Dans la fenêtre contextuelle qui apparaît, choisissez Mettre à jour le statut du contrôle pour confirmer que vous avez terminé de vérifier le contrôle.

Étape 6. Soumettre l'ensemble de contrôle vérifié au responsable de l'audit

Lorsque vous avez terminé de vérifier de tous les contrôles, soumettez-les à nouveau au responsable de l'audit pour lui faire savoir que vous avez terminé votre vérification.

Pour soumettre un ensemble de contrôle vérifié au responsable de l'audit

1. Sur la page Notifications, vérifiez la liste des ensembles de contrôles qui vous ont été assignés. Recherchez l'ensemble de contrôles que vous souhaitez soumettre au responsable de l'audit, puis choisissez le nom de l'évaluation associée.
2. Faites défiler la page jusqu'au tableau Ensembles de contrôles, sélectionnez l'ensemble de contrôles que vous souhaitez renvoyer au responsable de l'audit, puis choisissez Soumettre pour vérification.
3. Dans la fenêtre contextuelle qui apparaît, vous pouvez ajouter des commentaires généraux sur cet ensemble de contrôles avant de choisir Soumettre pour vérification.

Une fois que vous avez soumis le contrôle au responsable de l'audit, celui-ci peut consulter les commentaires que vous lui avez laissés.

Comment procéder ensuite ?

Vous pouvez continuer à en apprendre davantage sur les concepts présentés dans ce tutoriel. Voici quelques ressources recommandées :

- Vérification d'une évaluation : Vous présente la page d'évaluation où vous pouvez explorer les différents éléments d'une évaluation dans AWS Audit Manager.
- Vérifier les contrôles d'une évaluation et vérifier les preuves d'une évaluation : fournit des définitions de données pour vous aider à interpréter les contrôles et les preuves pour chaque évaluation.
- Concepts et terminologie AWS Audit Manager : fournit les définitions des concepts et de la terminologie utilisés dans Audit Manager.

Utilisation du tableau de bord d'Audit Manager

Avec le tableau de bord d'Audit Manager, vous pouvez visualiser les preuves non conformes dans vos évaluations actives. C'est un moyen pratique et rapide de suivre vos évaluations, de rester informé et de résoudre les problèmes de manière proactive. Par défaut, le tableau de bord fournit une vue agrégée de haut en bas de toutes vos évaluations actives. Grâce à cette vue, vous pouvez identifier visuellement les problèmes liés à vos évaluations sans avoir à passer au crible de grandes quantités de preuves individuelles.

Le tableau de bord est le premier écran que vous voyez lorsque vous vous connectez à la console Audit Manager. Il contient deux widgets qui affichent les données et les indicateurs de performance clés (KPI) les plus pertinents pour vous. À l'aide d'un filtre d'évaluation, vous pouvez affiner ces données afin de vous concentrer sur les KPI d'une évaluation spécifique. À partir de là, vous pouvez passer en revue les groupements de domaines de contrôle afin d'identifier les contrôles présentant le plus de preuves non conformes. Vous pouvez ensuite explorer les contrôles sous-jacents pour examiner et résoudre les problèmes.

> **Note**
>
> Si vous utilisez Audit Manager pour la première fois ou si aucune évaluation n'est active, aucune donnée n'est affichée dans le tableau de bord. Pour commencer, créez une évaluation. Cette étape marque le début de la collecte continue de preuves. Après une période de 24 heures, les données de preuve agrégées commenceront à apparaître dans le tableau de bord. Vous pouvez lire les sections suivantes pour savoir comment comprendre et interpréter ces données.

Cette page couvre les rubriques suivantes :

Rubriques

- Concepts et terminologie du tableau de bord
- Éléments du tableau de bord
- Que puis-je faire ensuite ?
- Résolution des problèmes

Concepts et terminologie du tableau de bord

Cette section couvre les informations importantes à connaître sur le tableau de bord d'Audit Manager avant de commencer à l'utiliser.

Autorisations et visibilité

Les responsables de l'audit et les délégués ont accès au tableau de bord. Cela signifie que ces deux catégories de personnes peuvent consulter les statistiques et les agrégats de toutes les évaluations actives de votre AWS compte. L'accès aux mêmes informations permet à toute votre équipe de se concentrer sur les mêmes KPI et objectifs.

Filtres

Audit Manager fournit un niveau de page the section called "Filtre d'évaluation" que vous pouvez appliquer à tous les widgets de votre tableau de bord.

Preuves non conformes

Le tableau de bord met en évidence les contrôles de vos évaluations qui contiennent des preuves de vérification de conformité et une conclusion de non-conformité. Les preuves du contrôle de conformité concernent les contrôles qui utilisent AWS Config ou AWS Security Hub en tant que type de source de données. Pour ce type de preuve, Audit Manager rapporte le résultat d'un contrôle de conformité directement depuis ces services. Si Security Hub indique un résultat d'échec ou AWS Config un résultat non conforme, Audit Manager classe les preuves comme non conformes.

Preuves non concluantes

Les preuves ne sont pas concluantes si un contrôle de conformité n'est pas disponible ou applicable. Par conséquent, aucune évaluation de conformité ne peut être effectuée. C'est le cas si un contrôle utilise AWS Config ou AWS Security Hub en tant que type de source de données mais que vous n'avez pas activé ces services. C'est également le cas si le contrôle utilise un type de source de données qui ne prend pas en charge les contrôles de conformité, tels que les preuves manuelles, les appels d'AWSAPI ouAWS CloudTrail.

Si les preuves ont le statut de vérification de conformité non applicable dans la console, elles sont classées comme non concluantes dans le tableau de bord.

Preuves conformes

Les preuves sont conformes si un contrôle de conformité n'a révélé aucun problème. Cela se produit si Security Hub signale un résultat de réussite ou si AWS Config signale un résultat conforme.

Domaines de contrôle

Le tableau de bord introduit le concept de domaine de contrôle. Vous pouvez considérer un domaine de contrôle comme une catégorie générale de contrôles qui n'est pas spécifique à un framework en particulier. Les groupements de domaines de contrôle sont l'une des fonctionnalités les plus puissantes du tableau de bord. Audit Manager met en évidence les contrôles de vos évaluations qui contiennent des preuves non conformes et les regroupe par domaine de contrôle. L'utilisation de cette fonctionnalité vous permet de concentrer vos efforts de remédiation sur des domaines spécifiques lorsque vous vous préparez à un audit.

> **Note**
>
> Un domaine de contrôle est différent d'un ensemble de contrôles. Un ensemble de contrôles est un regroupement de contrôles spécifique à un framework qui est généralement défini par un organisme de réglementation. Par exemple, le framework PCI DSS possède un ensemble de contrôles nommé Exigence 8 : identifier et authentifier l'accès aux composants du système. Cet ensemble de contrôles relève du domaine de contrôle de la gestion des identités et des accès.

Audit Manager classe les contrôles dans les domaines de contrôle suivants.

Nom du domaine de contrôle	Description de ce que ces contrôles régissent
Continuité des activités et planification des contingences	La manière dont vous établissez des processus protégeant les opérations commerciales critiques des effets des perturbations majeures du système et du réseau.
Gestion des modifications	La manière dont vous testez, approuvez, implémentez et documentez les modifications apportées à votre infrastructure cloud.

Nom du domaine de contrôle	Description de ce que ces contrôles régissent
Sécurité et confidentialité des données	La manière dont vous garantissez la confidentialité, la disponibilité et l'intégrité de vos données.
Gestion du développement et de la configuration	La manière dont vous maintenez votre infrastructure cloud dans un état souhaité et constant.
Gouvernance et supervision	La manière dont vous adaptez votre utilisation du cloud computing à vos obligations légales, réglementaires et éthiques.
Gestion des identités et des accès	La manière dont vous garantissez que les bons utilisateurs disposent de l'accès approprié à vos ressources technologiques.
Gestion des incidents	La manière dont vous établissez les responsabilités et les procédure s qui garantissent une réponse rapide et efficace aux incidents de sécurité.
Journalisation et surveillance	La manière dont vous examinez l'activité des utilisateurs pour détecter tout signe indiquant qu'une activité non autorisée a été tentée ou exécutée.
Gestion du réseau	La manière dont vous administrez et exploitez votre réseau de données à l'aide d'un système de gestion réseau.
Gestion du personnel	La manière dont vous évaluez et gérez les risques liés à la sécurité du personnel au niveau de l'organisation.
Sécurité physique	La manière dont vous détectez et prévenez les problèmes de sécurité physique dans vos installations.
Gestion des risques	La manière dont vous évaluez les risques et les pertes potentiels, et dont vous réduisez ou éliminez ces menaces.

Nom du domaine de contrôle	Description de ce que ces contrôles régissent
Gestion de la chaîne d'approvisionnement	La manière dont vous identifiez, évaluez et atténuez les risques associés aux produits informatiques, aux fournisseurs et aux chaînes d'approvisionnement.
Gestion des appareils utilisateur	La manière dont vous réduisez le risque de perte, d'endommagement ou de compromission du matériel informatique de vos employés.
Gestion de la vulnérabilité	La manière dont vous définissez, évaluez et corrigez toutes les vulnérabilités connues des actifs de votre infrastructure cloud.

Cohérence éventuelle des données

Les données du tableau de bord sont finalement cohérentes. Cela signifie que lorsque vous lisez des données du tableau de bord, il se peut que celles-ci ne reflètent pas instantanément les résultats d'une opération d'écriture ou de mise à jour récemment terminée. Si vous revérifiez dans les heures qui suivent, le tableau de bord devrait refléter les données les plus récentes.

Données provenant d'évaluations supprimées et inactives

Le tableau de bord affiche les données des évaluations actives. Si vous supprimez une évaluation ou passez son statut à inactif le jour même où vous consultez le tableau de bord, les données de cette évaluation sont incluses comme suit.

- Évaluations inactives : si l'Audit Manager a collecté des preuves pour votre évaluation avant que vous ne la rendiez inactive, ces preuves sont incluses dans le décompte du tableau de bord pour ce jour.
- Évaluations supprimées : si l'Audit Manager a collecté des preuves pour votre évaluation avant que vous ne les supprimiez, ces preuves ne sont pas incluses dans le décompte du tableau de bord pour ce jour.

Éléments du tableau de bord

Les sections suivantes couvrent les différents composants du tableau de bord.

Rubriques

- Filtre d'évaluation
- Aperçu quotidien
- Contrôles comportant des preuves non conformes regroupés par domaine de contrôle

Filtre d'évaluation

Vous pouvez utiliser le filtre d'évaluation pour vous concentrer sur une évaluation active spécifique.

Par défaut, le tableau de bord affiche des données agrégées pour toutes vos évaluations actives. Si vous souhaitez consulter les données d'une évaluation spécifique, vous devez appliquer un filtre d'évaluation. Il s'agit d'un filtre au niveau de la page qui s'applique à tous les widgets du tableau de bord.

Pour appliquer le filtre d'évaluation, sélectionnez une évaluation dans la liste déroulante en haut du tableau de bord. Cette liste affiche jusqu'à 10 de vos évaluations actives. Les évaluations les plus récentes apparaissent en premier. Si vous avez de nombreuses évaluations actives, vous pouvez commencer à saisir le nom d'une évaluation pour la retrouver rapidement. Une fois que vous avez sélectionné une évaluation, le tableau de bord affiche les données de cette évaluation uniquement.

Aperçu quotidien

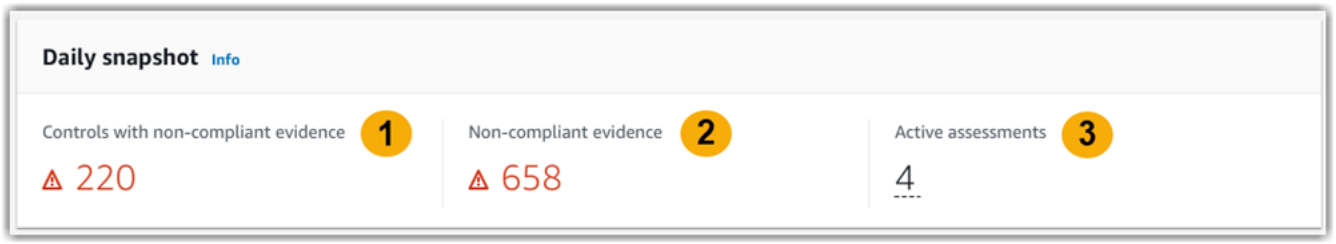
Ce widget affiche un aperçu de l'état de conformité actuel de vos évaluations actives.

L'aperçu quotidien reflète les dernières données collectées à la date indiquée en haut du tableau de bord. Les dates et heures affichées sur le tableau de bord sont exprimées en heure UTC (temps universel coordonné). Il importe de comprendre que ces chiffres sont des dénombrements quotidiens basés sur cet horodatage. Il ne s'agit pas d'une somme totale à ce jour.

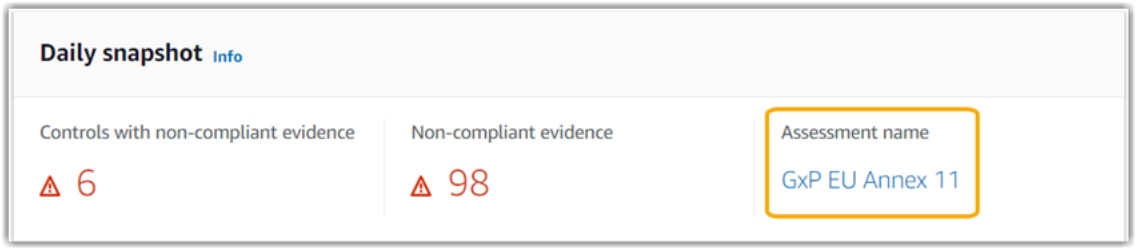
Par défaut, l'aperçu quotidien affiche les données suivantes pour toutes vos évaluations actives :

1. Contrôles comportant des preuves non conformes : nombre total de contrôles associés à des preuves non conformes.
2. Preuves non conformes - Le nombre total de preuves de contrôle de conformité aboutissant à une conclusion non conforme.

3. Évaluations actives : nombre total de vos évaluations actives. Choisissez ce numéro pour voir les liens vers ces évaluations.



Les données instantanées quotidiennes changent en fonction de the section called "Filtre d'évaluation" ce que vous appliquez. Lorsque vous spécifiez une évaluation, les données reflètent les chiffres quotidiens pour cette évaluation uniquement. Dans ce cas, l'instantané quotidien indique le nom de l'évaluation que vous avez spécifiée. Vous pouvez choisir le nom de l'évaluation pour l'ouvrir.

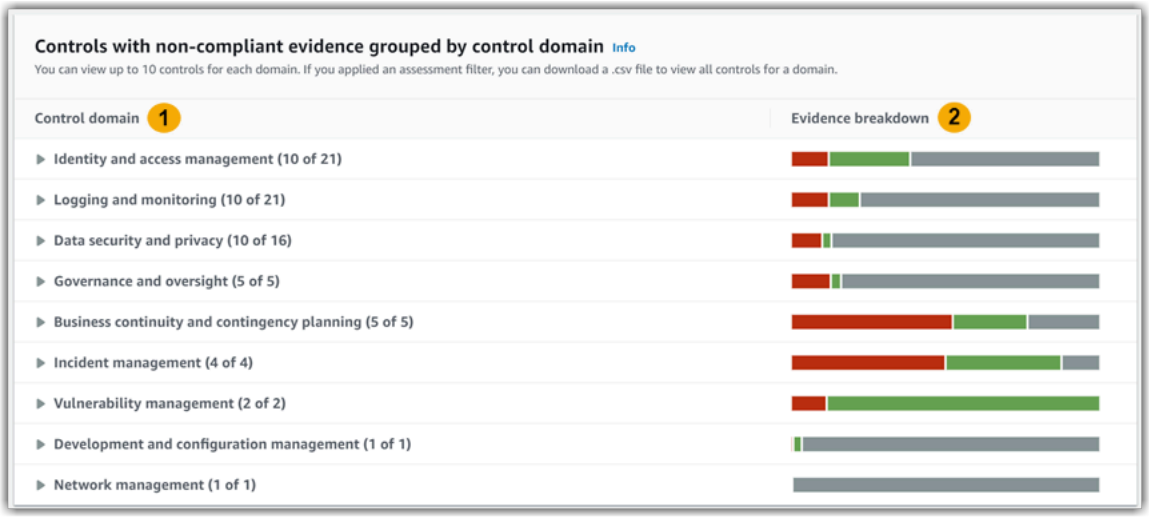


Contrôles comportant des preuves non conformes regroupés par domaine de contrôle

Vous pouvez utiliser ce widget pour identifier les contrôles présentant le plus de preuves non conformes.

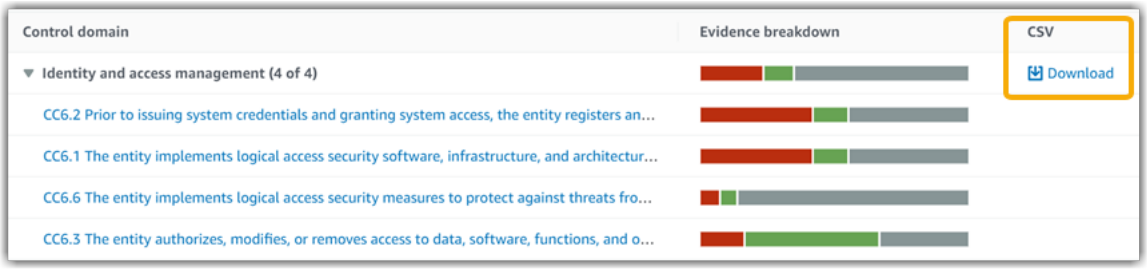
Par défaut, le widget affiche les données suivantes pour toutes vos évaluations actives :

1. Domaine de contrôle : liste control domains des domaines associés à vos évaluations actives.
2. Répartition des preuves — Un graphique à barres qui montre une ventilation de l'état de conformité des preuves.



Pour développer un domaine de contrôle, choisissez la flèche à côté de son nom. Lorsqu'elle est étendue, la console affiche jusqu'à 10 commandes pour chaque domaine. Ces contrôles sont classés en fonction du nombre total le plus élevé de preuves non conformes.

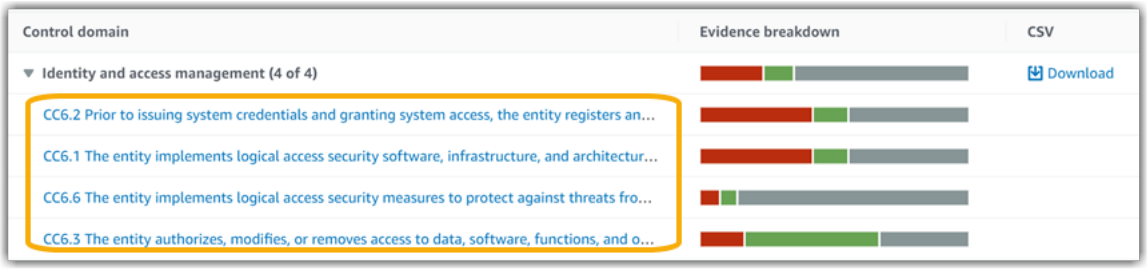
Les données de ce widget changent en fonction de celles the section called "Filtre d'évaluation" que vous appliquez. Lorsque vous spécifiez une évaluation, vous ne voyez que les données de cette évaluation. En outre, vous pouvez également télécharger un fichier .csv pour chaque domaine de contrôle disponible dans l'évaluation.



Le fichier .csv inclut la liste complète des contrôles du domaine qui sont associés à des preuves non conformes. L'exemple suivant montre les colonnes de données .csv avec des valeurs fictives.

	A	B	C	D	E	F	G
1	Date and Time	AssessmentID	AsessmentName	ControlId	ControlName	ControlDescription	DataSource
2	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	abcdefgh-1234-bcde-5678-cdefghijklmn	Control 1	Description of control 1	Manual
3	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	12345678-abcd-9012-bcde-345678901234	Control 2	Description of control 2	Manual
4	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	bcdefghi-2345-cdef-3456-defghijklmno	Control 3	Description of control 3	AWS Config, AWS Security Hub
5	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	23456789-bcde-0123-cdef-456789012345	Control 4	Description of control 4	Manual
6	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	cdefghij-3456-defg-4567-efghijklmnop	Control 5	Description of control 5	AWS Config
7	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	34567890-cdef-1234-defg-567890123456	Control 6	Description of control 6	Manual
8	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	defghijk-4567-efgh-5678-fghijklmnopq	Control 7	Description of control 7	AWS Config
9	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	45678901-defg-2345-efgh-678901234567	Control 8	Description of control 8	AWS Security Hub
10	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	efghijkl-5678-fghi-6789-ghijklmnopqr	Control 9	Description of control 9	Manual
11	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	56789012-efgh-3456-fghi-789012345678	Control 10	Description of control 10	Manual
12	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	fghijklm-6789-ghij-7890-hijklmnopqrs	Control 11	Description of control 11	Manual
13	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	67890123-fghi-4567-ghij-890123456789	Control 12	Description of control 12	Manual
14	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	ghijklmn-7890-hijk-8901-ijklmnopqrst	Control 13	Description of control 13	AWS Config, AWS Security Hub
15	Thu Oct 21 2021 21:31:05 GMT-0700	12345678-abcd-2345-bcde-345678901234	My assessment	78901234-ghij-5678-hijk-901234567890	Control 14	Description of control 14	Manual
16							

Enfin, lorsque vous appliquez un filtre d'évaluation, les noms de contrôle sous chaque domaine sont associés à des liens hypertextes. Choisissez n'importe quel contrôle pour ouvrir la page des détails du contrôle dans l'évaluation spécifiée.



> **Tip**
>
> En utilisant la page des détails du contrôle comme point de départ, vous pouvez passer d'un niveau de détail à l'autre.
>
> 1. Page des détails du contrôle - Sur cette page, l'onglet Dossiers de preuves répertorie les dossiers quotidiens de preuves collectés par Audit Manager pour ce contrôle. Pour plus de détails, choisissez un dossier.
> 2. Dossier de preuves : vous pouvez ensuite consulter le résumé du dossier et la liste des preuves qu'il contient. Pour obtenir plus de détails, sélectionnez un élément de preuve individuel.
> 3. Preuve individuelle - Enfin, vous pouvez explorer les détails des preuves individuelles. Cela inclut tous les attributs et données de ressources applicables aux preuves. Il s'agit du niveau de preuve le plus granulaire.

Que puis-je faire ensuite ?

Voici les prochaines étapes que vous pouvez suivre après avoir consulté le tableau de bord.

- Téléchargez un fichier .csv : trouvez le domaine d'évaluation et de contrôle sur lequel vous souhaitez vous concentrer, et téléchargez la liste complète des contrôles associés présentant des preuves non conformes.
- Révision d'un contrôle : une fois que vous avez identifié un contrôle nécessitant une correction, vous pouvez le réviser.
- Déléguer un contrôle pour révision : si vous avez besoin d'aide pour réviser un contrôle, vous pouvez déléguer un ensemble de contrôles pour révision.

- Modifier votre évaluation : si vous souhaitez modifier le champ d'application d'une évaluation active, vous pouvez modifier l'évaluation.
- Mettez à jour le statut de votre évaluation — Si vous souhaitez arrêter de collecter des preuves d'évaluation, vous pouvez modifier le statut de l'évaluation en inactif.

Résolution des problèmes

Pour trouver des réponses aux questions et problèmes courants, voir Résolution des problèmes liés au tableau de bord dans la section Résolution des problèmes de ce guide.

Évaluations dans AWS Audit Manager

Une évaluation Audit Manager est basée sur un cadre, qui est un regroupement de contrôles. En utilisant un cadre comme point de départ, vous pouvez créer une évaluation qui recueille des preuves pour effectuer des contrôles dans ce cadre. Dans votre évaluation, vous pouvez également définir le périmètre de votre audit. Cela inclut la spécification des Comptes AWS et des services pour lesquels vous souhaitez recueillir des preuves.

Vous pouvez créer une évaluation à partir de n'importe quel framework. Vous pouvez soit utiliser un cadre standard fourni par Audit Manager, soit créer une évaluation à partir d'un cadre personnalisé que vous avez créé vous-même. Les frameworks standard contiennent des ensembles de contrôle prédéfinis qui prennent en charge une norme ou une réglementation de conformité spécifique. En revanche, les frameworks personnalisés contiennent des contrôles que vous pouvez personnaliser et regrouper en fonction de vos exigences en matière d'audit interne. Pour plus d'informations sur les différences entre les cadres standard et personnalisés, veuillez consulter Cadres dans la section Concepts et terminologie du présent guide.

Lorsque vous créez une évaluation, cela lance la collecte continue de preuves. Au moment de procéder à un audit, vous ou un délégué pouvez examiner ces preuves, puis les ajouter à un rapport d'évaluation.

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

Rubriques

- Création d'une évaluation
- Accès à vos évaluations dans AWS Audit Manager
- Modification d'une évaluation
- Vérification d'une évaluation

- Vérification des contrôles dans le cadre d'une évaluation
- Examen des preuves dans le cadre d'une évaluation
- Ajouter des preuves manuelles dans AWS Audit Manager
- Génération de rapports d'évaluation
- Modification du statut d'une évaluation en statut inactif
- Suppression d'une évaluation

Création d'une évaluation

Cette rubrique s'appuie sur le tutoriel Mise en route : Création d'une évaluation. Elle contient des instructions détaillées sur la façon de créer une évaluation à partir d'un cadre. Suivez ces étapes pour créer une évaluation et commencer la collecte continue de preuves.

Tâches

- Étape 1 : Indiquer les détails de l'évaluation
- Étape 2 : Indiquer les Comptes AWS concernés
- Étape 3 : Indiquer Services AWS concernés
- Étape 4 : Indiquer les responsables de l'audit
- Étape 5 : Vérification et création
- Que puis-je faire ensuite ?

Étape 1 : Indiquer les détails de l'évaluation

Commencez par sélectionner un cadre et fournissez des informations de base pour votre évaluation.

Pour indiquer les détails de l'évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations, puis choisissez Créer une évaluation.
   - Sinon, dans le panneau de navigation, sélectionnez Mise en route, puis sélectionnez Créer une évaluation.
3. Sous Nom de l'évaluation, saisissez un nom pour votre évaluation.

4. (Facultatif) Sous Description de l'évaluation, saisissez une description pour votre évaluation.
5. Sous Destination des rapports d'évaluation, sélectionnez un compartiment Amazon S3 existant dans lequel vous souhaitez enregistrer vos rapports d'évaluation.

> **Tip**
>
> La destination du rapport d'évaluation par défaut est basée sur les paramètres de votre Audit Manager. Pour plus d'informations, veuillez consulter AWS Audit Manager Paramètres, Destination du rapport d'évaluation. Si vous préférez, vous pouvez créer et utiliser plusieurs compartiments S3 pour vous aider à organiser vos rapports d'évaluation.

6. Sous Cadres, sélectionnez le cadre à partir duquel vous souhaitez créer votre évaluation. Vous pouvez également utiliser la barre de recherche pour rechercher une structure par son nom, ou par norme ou réglementation de conformité.

> **Tip**
>
> Pour en savoir plus sur un cadre, choisissez le nom du cadre. Cette action ouvre la page récapitulative du cadre. Sur cette page, vous pouvez consulter le contenu de ce cadre. Cela inclut les contrôles et les sources de données du cadre.

7. Sous Balises, choisissez Ajouter une nouvelle balise pour associer une balise à votre évaluation. Vous pouvez indiquer une clé et une valeur pour chaque balise. La clé de balise est obligatoire et peut être utilisée comme critère de recherche lorsque vous recherchez cette évaluation. Pour plus d'informations sur les balises dans l'Audit Manager, veuillez consulter Balisage de ressources AWS Audit Manager.
8. Choisissez Suivant.

> **Note**
>
> Il est important de vous assurer que votre évaluation recueille les preuves appropriées pour un cadre donné. Avant de commencer la collecte de preuves, nous vous recommandons de passer en revue les exigences du cadre que vous avez choisi. Ensuite, validez ces exigences par rapport à vos paramètres de règle AWS Config actuels. Pour vous assurer que vos paramètres de règle sont conformes aux exigences du cadre, vous pouvez mettre à jour la règle dans AWS Config.

Supposons, par exemple, que vous créez une évaluation pour CIS v1.2.0. Ce framework possède un contrôle nommé 1.9 : assurez-vous que la politique de mot de passe IAM nécessite une longueur minimale de 14 ou plus. Dans AWS Config, la règle iam-password-policy contient un paramètre `MinimumPasswordLength` qui vérifie la longueur du mot de passe. La valeur par défaut de ce paramètre est de 14 caractères. Par conséquent, la règle s'aligne sur les exigences de contrôle. Si vous n'utilisez pas la valeur de paramètre par défaut, assurez-vous que la valeur que vous utilisez est égale ou supérieure aux 14 caractères requis par CIS v1.2.0. Vous trouverez les détails des paramètres par défaut pour chaque règle gérée dans la documentation AWS Config.

Étape 2 : Indiquer les Comptes AWS concernés

Vous pouvez spécifier plusieurs Comptes AWS pour qu'ils soient inclus dans le champ d'une évaluation. Audit Manager prend en charge plusieurs comptes grâce à l'intégration à AWS Organizations. Cela signifie que les évaluations Audit Manager peuvent être effectuées sur plusieurs comptes, les preuves collectées étant consolidées dans un compte d'administrateur délégué. Pour activer Organisations dans Audit Manager, veuillez consulter Activer AWS Organizations (facultatif).

> **Note**
>
> Audit Manager peut prendre en charge jusqu'à 150 comptes dans le cadre d'une évaluation. Si vous essayez d'inclure plus de 150 comptes, la création de l'évaluation risque d'échouer.

Pour spécifier Comptes AWS dans le champ d'application

1. Sous Comptes AWS, sélectionnez les éléments Comptes AWS que vous souhaitez inclure dans le champ de votre évaluation.
   - Si vous avez activé Organisations dans Audit Manager, plusieurs comptes sont affichés. Vous pouvez sélectionner un ou plusieurs comptes dans la liste. Vous pouvez également rechercher un compte à l'aide de son nom, de son identifiant ou de son adresse e-mail.
   - Si vous n'avez pas activé Organisations dans Audit Manager, seul votre compte actuel Compte AWS est répertorié.
2. Choisissez Next (Suivant).

> **Note**
>
> Lorsqu'un compte concerné est supprimé de votre organisation, Audit Manager ne collecte plus de preuves pour ce compte. Cependant, le compte continue d'apparaître dans votre évaluation sous l'onglet Comptes AWS. Pour supprimer le compte de la liste des comptes concernés, vous pouvez modifier l'évaluation. Le compte supprimé n'apparaît plus dans la liste lors de la modification et vous pouvez enregistrer vos modifications sans que ce compte soit concerné.

Étape 3 : Indiquer Services AWS concernés

Le cadre que vous avez sélectionné précédemment définit le cadre Services AWS pour lequel Audit Manager surveille et collecte des preuves. Si une liste Service AWS n'est pas sélectionnée, ou si elle est sélectionnée mais que vous ne l'avez pas activée dans votre environnement, Audit Manager ne collecte aucune preuve à partir des ressources liées à ce service.

Vous pouvez définir le Services AWS concerné comme suit.

Pour les évaluations créées à partir de cadres standard

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir d'un cadre standard, la liste des Services AWS concernés est sélectionnée par défaut. Cette liste ne peut pas être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework standard. Si le cadre standard que vous avez sélectionné ne contient que des contrôles manuels, aucun Services AWS n'est concerné dans votre évaluation et vous ne pouvez ajouter aucun service à votre évaluation.

Pour continuer, consultez la liste et choisissez Suivant.

> **Tip**
>
> Si vous devez modifier la liste des services concernés, vous pouvez le faire à l'aide de l'API Créer une évaluation fournie par Audit Manager.
> Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour les évaluations créées à partir de cadres personnalisés

Si vous avez sélectionné un cadre personnalisé à l'étape 1, vous pouvez consulter et modifier la liste des Services AWS des cadres concernés par votre évaluation. Si le cadre personnalisé que vous avez sélectionné contient uniquement des contrôles manuels, tous les Services AWS sont affichés mais aucun n'est sélectionné. Vous pouvez sélectionner zéro ou plusieurs services à inclure dans le champ d'application de votre évaluation.

Pour spécifier Services AWS dans le champ d'application (pour les évaluations créées à partir de cadres personnalisés uniquement)

1. Sous Services AWS, sélectionnez les services à inclure dans votre évaluation. Vous pouvez trouver des services supplémentaires en utilisant la barre de recherche pour effectuer une recherche par service, catégorie ou description. Pour ajouter un service, cochez la case en regard du nom du service. Pour supprimer un service, décochez la case.
2. Lorsque vous avez terminé la sélection Services AWS, choisissez Suivant.

Étape 4 : Indiquer les responsables de l'audit

Dans cette étape, vous indiquez les responsables de l'audit pour votre évaluation. Les responsables de l'audit sont les personnes de votre lieu de travail, généralement issues des équipes GRC, SecOps ou DevOps, qui sont chargées de gérer l'évaluation de l'Audit Manager. Nous leur recommandons d'utiliser la politique d'accès AWSAuditManagerAdministratorAccess.

Pour indiquer les responsables de l'audit

1. Sous Responsables de l'audit, consultez la liste actuelle des responsables de l'audit. La colonne Responsable de l'audit affiche les ID utilisateur et les rôles. La colonne Compte AWS affiche leCompte AWS associé à ce responsable d'audit.
2. Les responsables de l'audit pour lesquels une case est cochée sont inclus dans votre évaluation. Décochez la case correspondant à tout responsable de l'audit afin de le supprimer de l'évaluation. Vous pouvez trouver d'autres responsables d'audit en utilisant la barre de recherche pour effectuer une recherche par nom ou Compte AWS.
3. Lorsque vous avez terminé, choisissez Suivant.

Étape 5 : Vérification et création

Vérifiez les informations de votre évaluation. Pour modifier les informations d'une étape, choisissez Modifier. Lorsque vous avez terminé, choisissez Créer une évaluation.

Cette action lance la collecte continue de preuves pour votre évaluation. Une fois que vous avez créé une évaluation, la collecte de preuves se poursuit jusqu'à ce que vous passiez le statut de l'évaluation à inactif. Vous pouvez également arrêter la collecte de preuves pour un contrôle précis en faisant passer le statut du contrôle à inactif.

> **Note**
>
> Les preuves automatisées sont disponibles 24 heures après la création de votre évaluation. Audit Manager collecte automatiquement des preuves à partir de plusieurs sources de données, et la fréquence de cette collecte de preuves est basée sur le type de preuves. Pour de plus amples informations, veuillez consulter Fréquence de collecte des preuves dans le présent guide.

Que puis-je faire ensuite ?

Une fois que vous aurez créé votre évaluation, vous pourrez approfondir vos connaissances concernant les points suivants :

- Accéder à une évaluation
- Vérification d'une évaluation
- Modification d'une évaluation
- Vérification des contrôles dans le cadre d'une évaluation
- Examen des preuves dans le cadre d'une évaluation
- Télécharger des preuves manuelles dans une évaluation
- La délégation dans AWS Audit Manager
- Génération de rapports d'évaluation
- Modifier le statut d'une évaluation
- Suppression d'une évaluation
- Résolution des problèmes liés aux évaluations et à la collecte de preuves

Accès à vos évaluations dans AWS Audit Manager

Vous pouvez consulter toutes vos évaluations sur la page Évaluations de la console Audit Manager. À partir de là, vous pouvez également modifier une évaluation, supprimer une évaluation ou créer une évaluation.

Vous pouvez également consulter vos évaluations à l'aide de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

Audit Manager console

Pour consulter vos évaluations (console)

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Évaluations pour afficher la liste de vos évaluations actives et passées. Vous pouvez également utiliser la barre de recherche pour rechercher une évaluation.
3. Choisissez un nom d'évaluation pour ouvrir une page récapitulative, où vous pouvez consulter les détails de cette évaluation.

AWS CLI

Pour afficher vos évaluations (CLI)

Pour consulter les évaluations dans Audit Manager, exécutez la commande list-assessments. Vous pouvez utiliser la sous-commande `--status` pour afficher les évaluations actives ou inactives.

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

```
aws auditmanager list-assessments --status INACTIVE
```

Audit Manager API

Pour consulter vos évaluations (API)

Pour consulter les évaluations dans Audit Manager, utilisez l'opération Répertorier les évaluations. Vous pouvez utiliser l'attribut statut pour afficher les évaluations actives ou inactives.

Pour plus d'informations, choisissez l'un des liens précédents pour en lire davantage dans le Guide de référence de l'API AWS Audit Manager. Il inclut des informations sur l'utilisation du fonctionnement et des paramètres `ListAssessments` dans l'un des SDK AWS spécifiques au langage.

Modification d'une évaluation

Vous pouvez modifier vos évaluations actives dans Audit Manager pour modifier des informations telles que la description, le champ d'application, les responsables de l'audit et la destination du rapport d'évaluation.

Tâches

- Étape 1 : Modifier les détails de l'évaluation
- Étape 2 : Modifier Comptes AWS dans le champ d'application
- Étape 3 : Modifier Services AWS dans le champ d'application
- Étape 4 : Modifier les responsables d'audit
- Étape 5 : Vérification et sauvegarde

Étape 1 : Modifier les détails de l'évaluation

Procédez comme suit pour modifier les détails de votre évaluation.

Pour modifier une évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations pour afficher votre liste actuelle d'évaluations.
3. Sélectionnez une évaluation, puis choisissez Modifier.
   - Sinon, vous pouvez ouvrir l'évaluation, puis sélectionner Modifier en haut à droite de la page.
4. Sous Modifier les détails de l'évaluation, modifiez le nom, la description et la destination du rapport d'évaluation.
5. Choisissez Next (Suivant).

> **Tip**
>
> Pour modifier les balises d'une évaluation, ouvrez l'évaluation et choisissez le Onglet Balises. Vous pouvez y afficher et modifier les balises associées à l'évaluation.

Étape 2 : Modifier Comptes AWS dans le champ d'application

Au cours de cette étape, vous pouvez modifier la liste des comptes inclus dans le périmètre de votre évaluation.

Audit Manager prend en charge plusieurs comptes grâce à l'intégration à AWS Organizations. Cela signifie que les évaluations Audit Manager peuvent être effectuées sur plusieurs comptes, les preuves collectées étant consolidées dans un compte d'administrateur délégué. Pour ajouter ou modifier l'administrateur délégué pour Audit Manager, veuillez consulter paramètres AWS Audit Manager, Administrateur délégué.

> **Note**
>
> Audit Manager peut prendre en charge jusqu'à 150 comptes dans le cadre d'une évaluation. Si vous essayez d'inclure plus de 150 comptes, la création de l'évaluation risque d'échouer.

Pour modifier Comptes AWS dans le champ d'application

1. Sous Modifier Comptes AWS dans le champ d'application, sélectionnez des comptes AWS supplémentaires. Vous pouvez également supprimer des comptes en les retirant de la liste.
2. Choisissez Next (Suivant).

Étape 3 : Modifier Services AWS dans le champ d'application

Cette étape indique pour quel Audit Manager Services AWS surveille et collecte des preuves. Si un Service AWS répertorié n'est pas sélectionné, ou s'il est sélectionné mais que vous ne l'avez pas activé dans votre environnement, Audit Manager ne collecte pas de preuves à partir des ressources liées à ce service.

Vous pouvez consulter et modifier le Services AWS dans le champ d'application comme suit.

Pour les évaluations créées à partir de cadres standard

Lorsque vous utilisez la console Audit Manager pour modifier une évaluation créée à partir d'un cadre standard, vous pouvez consulter la liste des Services AWS dans le champ d'application, mais vous ne pouvez pas modifier cette liste. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous, conformément à la conception du cadre standard. Si l'évaluation a été créée à l'aide d'un cadre contenant uniquement des contrôles manuels, aucun Services AWS n'est concerné par votre évaluation et vous ne pouvez ajouter aucun service.

Pour continuer, consultez la liste et choisissez Suivant.

> **Tip**
>
> Si vous devez modifier la liste des services concernés par une évaluation existante, vous pouvez le faire à l'aide de l'API Mettre à jour l'évaluation fournie par Audit Manager.

Pour les évaluations créées à partir de cadres personnalisés

Si vous avez créé l'évaluation à partir d'un cadre personnalisé, vous pouvez modifier les éléments Services AWS concernés par votre évaluation. Vous pouvez sélectionner zéro ou plusieurs services à inclure dans le champ d'application de votre évaluation.

Pour modifier Services AWS concernés (pour les évaluations créées à partir de cadres personnalisés uniquement)

1. Sous Modifier Services AWS dans le champ d'application, sélectionnez l'option Services AWS supplémentaire si nécessaire. Vous pouvez également supprimer des services en les retirant de la liste.
2. Choisissez Next (Suivant).

Étape 4 : Modifier les responsables d'audit

Vous pouvez également modifier les responsables de l'audit de votre évaluation. Les responsables de l'audit sont les personnes de votre lieu de travail, généralement issues des équipes GRC, SecOps ou DevOps, qui sont chargées de gérer l'évaluation de l'Audit Manager. Leurs tâches incluent la délégation des ensembles de contrôle pour examen et la génération de rapports d'évaluation. Nous vous recommandons d'utiliser la politique AWSAuditManagerAdministratorAccess.

Pour modifier les responsables de l'audit

1. Sélectionnez les nouveaux responsables de l'audit à ajouter à l'évaluation. Pour supprimer les responsables de l'audit, supprimez-les de la liste.
2. Choisissez Next (Suivant).

Étape 5 : Vérification et sauvegarde

Vérifiez les informations de votre évaluation. Pour modifier les informations d'une étape, choisissez Modifier. Lorsque vous avez terminé les modifications, choisissez Enregistrer les modifications pour confirmer vos modifications.

> **Note**
>
> Une fois que vous avez terminé vos modifications, les modifications apportées à l'évaluation prennent effet à 00h00 UTC le jour suivant.

Vérification d'une évaluation

Après avoir créé des évaluations dans Audit Manager, vous pouvez les ouvrir et les consulter à tout moment.

Pour ouvrir et vérifier une évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Évaluations pour afficher la liste de vos évaluations.
3. Choisissez le nom de l'évaluation pour l'ouvrir.

Lorsque vous ouvrez une évaluation, une page récapitulative contenant plusieurs sections s'affiche. Les sections de cette page et leur contenu sont décrits comme suit.

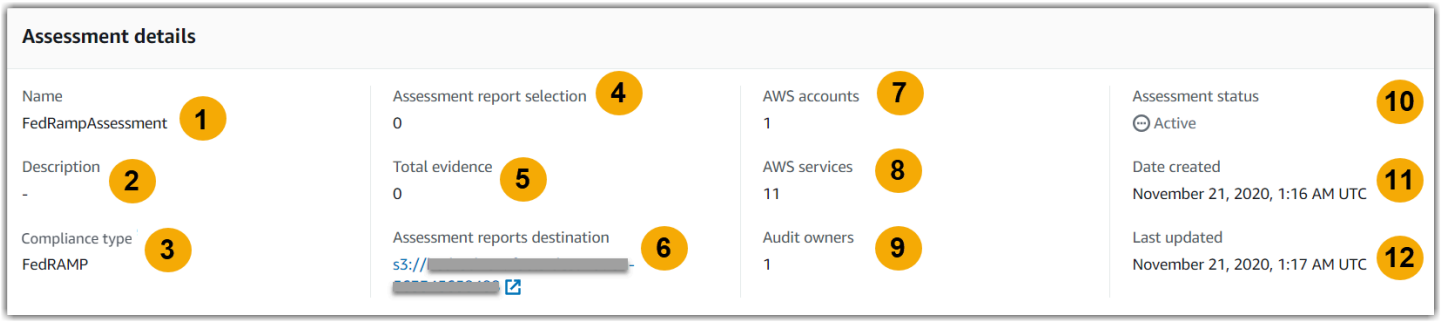
Sections de la page d'évaluation

- Détails de l'évaluation

- Onglet Contrôles
- Onglet de sélection du rapport d'évaluation
- Onglet Comptes AWS
- Onglet Services AWS
- Onglet des responsables de l'Audit
- Onglet Balises
- Onglet Journal des modifications

Détails de l'évaluation

La section Détails de l'évaluation fournit une vue d'ensemble de l'évaluation.



Il contient les informations suivantes :

1. Nom : nom que vous avez fourni pour l'évaluation.
2. Description : description facultative que vous avez fournie pour l'évaluation.
3. Type de conformité : norme ou réglementation de conformité prise en charge par l'évaluation.
4. Sélection du rapport d'évaluation : nombre d'éléments de preuve que vous choisissez d'inclure dans le rapport d'évaluation.
5. Total des preuves : nombre total d'éléments de preuve collectés pour cette évaluation.
6. Destination des rapports d'évaluation : le compartiment Amazon S3 dans lequel Audit Manager enregistre le rapport d'évaluation.
7. Comptes AWS— Le nombre de Comptes AWS qui entrent dans le champ d'application de cette évaluation.
8. Services AWS— Le nombre de Services AWS qui entrent dans le champ d'application de cette évaluation.

9. Responsables de l'audit : nombre de responsables de l'audit pour cette évaluation.
10. Statut de l'évaluation — Le statut de l'évaluation.
    - Actif : indique que l'évaluation recueille actuellement des preuves. Les évaluations nouvellement créées ont ce statut.
    - Inactif : indique que l'évaluation ne collecte plus de preuves. Pour plus d'informations sur les évaluations inactives, veuillez consulter Modification du statut d'une évaluation en statut inactif.
11. Date de création : date à laquelle l'évaluation a été créée.
12. Dernière mise à jour : date à laquelle cette évaluation a été modifiée pour la dernière fois.

Onglet Contrôles

L'onglet Contrôles affiche un résumé des contrôles de l'évaluation, ainsi qu'une liste complète de ces contrôles. Chaque évaluation peut contenir plusieurs ensembles de contrôles, et chaque ensemble de contrôles contient plusieurs contrôles. Les contrôles et les ensembles de contrôles sont organisés de manière à correspondre à la disposition définie dans la norme ou le règlement de conformité associé.

Sous Résumé du statut des contrôles, vous pouvez consulter un résumé des contrôles pour cette évaluation. Le résumé comprend les informations suivantes :

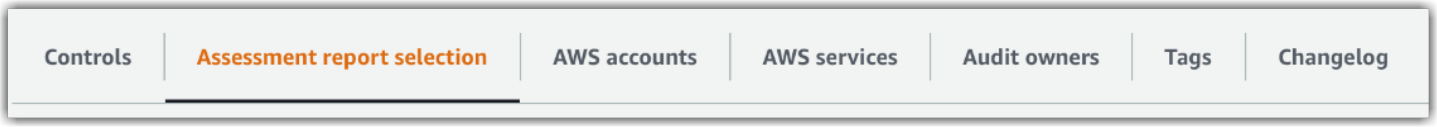
- Nombre total de contrôles : nombre total de contrôles inclus dans cette évaluation.
- Vérifié : nombre de contrôles qui ont été vérifiés par le responsable de l'audit ou son délégué.
- En cours de vérification : nombre de contrôles actuellement en cours de vérification.
- Inactif : nombre de contrôles qui ne collectent plus activement de preuves.

Dans le tableau Ensembles de contrôles, une liste de contrôles est affichée et regroupée par ensemble de contrôles. Vous pouvez étendre ou réduire les contrôles de chaque ensemble de contrôles. Vous pouvez également effectuer une recherche par nom de contrôle si vous souhaitez rechercher un contrôle en particulier. Les colonnes de données suivantes apparaissent dans le tableau Contrôles regroupés par ensembles de contrôles :

- Contrôles regroupés par ensembles de contrôles : nom de l'ensemble de contrôles.

- Statut du contrôle : il s'agit du statut du contrôle.
  - En cours de vérification indique que ce contrôle n'a pas encore été vérifié. Des preuves sont toujours en cours de collecte pour ce contrôle, et vous pouvez charger des preuves manuelles. Il s'agit du statut par défaut.
  - Vérifié indique que les preuves de ce contrôle ont été vérifiées. Cependant, les preuves sont toujours en cours de collecte et vous pouvez télécharger des preuves manuelles.
  - Inactif indique que la collecte automatique de preuves est interrompue pour ce contrôle. Vous ne pouvez plus télécharger de preuves manuelles.
- Délégué à : l'examinateur de ce contrôle, s'il a été attribué à un délégué pour vérification.
- Total des preuves : nombre d'éléments de preuve collectés pour ce contrôle.

Onglet de sélection du rapport d'évaluation



Cet onglet affiche la liste des preuves à inclure dans le rapport d'évaluation, regroupée par dossiers de preuves. Ces dossiers de preuves sont organisés et nommés en fonction de la date à laquelle ils ont été créés. Vous pouvez parcourir ces dossiers et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Vous pouvez également utiliser la barre de recherche pour effectuer une recherche par nom de contrôle ou nom de dossier de preuves. Le nombre total d'éléments de preuve ajoutés au rapport d'évaluation est résumé dans la section Détails de l'évaluation en haut de la page.

Le tableau de sélection du rapport d'évaluation présente une liste de dossiers de preuves contenant les données suivantes :

- Dossier de preuves : nom du dossier de preuves. Le nom du dossier est basé sur la date à laquelle les preuves ont été collectées.
- Preuves sélectionnées : nombre d'éléments de preuve contenus dans le dossier qui sont inclus dans le rapport d'évaluation.
- Nom du contrôle : nom du contrôle associé à ce dossier de preuves.

Pour plus d'informations sur l'ajout de preuves à un rapport d'évaluation, veuillez consulterGénération de rapports d'évaluation.

Onglet Comptes AWS

Cet onglet affiche la liste des Comptes AWS entrant dans le champ d'application de l'évaluation. Le nombre total de comptes est résumé dans la section Détails de l'évaluation en haut de la page.

Le tableau Comptes AWS présente une liste de comptes contenant les données suivantes :

- ID du compte : l'ID du Compte AWS.
- Nom du compte : le nom du Compte AWS.
- E-mail : l'adresse e-mail associée au Compte AWS.

Onglet Services AWS

Cet onglet affiche la liste des Services AWS entrant dans le champ d'application de l'évaluation. En d'autres termes, il s'agit de Services AWS pour lesquels votre évaluation recueille des preuves.

Le nombre total de services est résumé dans la section Détails de l'évaluation en haut de la page.

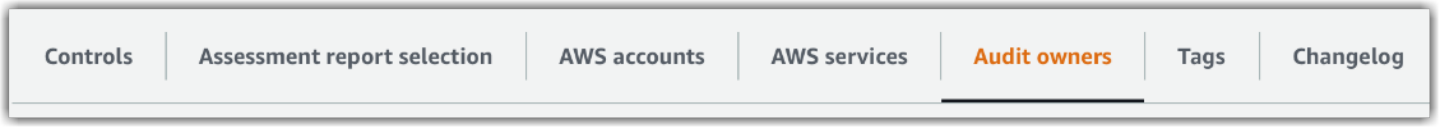
Le tableau Services AWS présente une liste de services avec les données suivantes :

- Service AWS : Le nom de Service AWS.
- Catégorie : catégorie de service, telle que le calcul ou la base de données.

Audit Manager effectue des évaluations des ressources pour les services figurant dans ce tableau. Par exemple, si Amazon S3 est répertorié, Audit Manager peut collecter des preuves concernant vos compartiments S3. Les preuves exactes collectées sont déterminées par la source de données d'un contrôle. Par exemple, si le type de source de données est AWS Config et que le mappage des sources de données est une règle AWS Config (telle que `s3-bucket-public-write-prohibited`), Audit Manager collecte le résultat de cette évaluation des règles à titre de preuve. Pour plus d'informations, veuillez consulter Quelle est la différence entre un service inclus et un type de source de données ? dans ce guide.

> **Note**
>
> Si votre évaluation a été créée dans la console à partir d'un cadre standard, Audit Manager a sélectionné les services pour vous et a mappé leurs sources de données conformément aux exigences du cadre. Si le cadre standard ne contient que des contrôles manuels, aucun Services AWS n'est concerné. Si vous devez modifier la liste des services concernés, vous pouvez utiliser l'API Mettre à jour l'évaluation.

Onglet des responsables de l'Audit

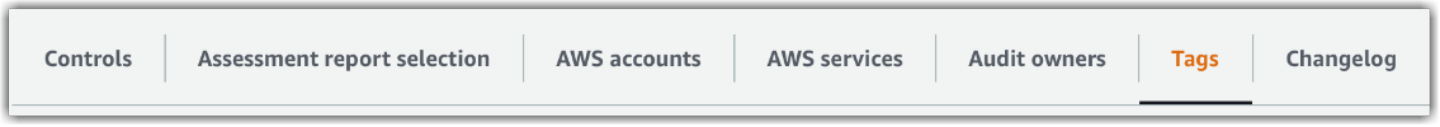


Cet onglet affiche les responsables de l'audit pour l'évaluation. Le nombre total de services est résumé dans la section Détails de l'évaluation en haut de la page.

Le tableau des Responsables de l'audit présente une liste de comptes contenant les données suivantes :

- Responsable de l'audit : nom du responsable de l'audit.
- Compte AWS :l'adresse e-mail associée au responsable de l'audit.

Onglet Balises



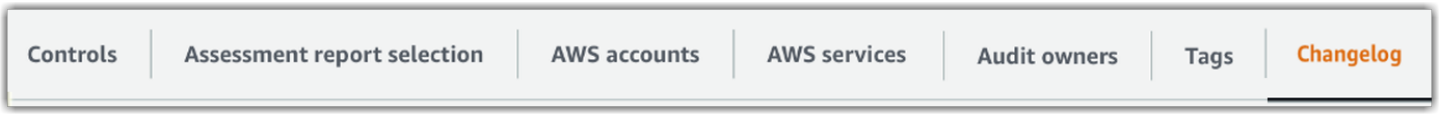
Cet onglet affiche la liste des balises héritées du cadre utilisées pour créer cette évaluation. Le nombre total de services est résumé dans la section Détails de l'évaluation en haut de la page.

Le tableau Balises présente une liste de balises contenant les données suivantes :

- Clé : la clé de la balise par exemple, une norme de conformité, une réglementation ou une catégorie.
- Valeur : valeur de la balise.

Pour plus d'informations sur les balises dans l'Audit Manager, veuillez consulter Balisage de ressources AWS Audit Manager.

Onglet Journal des modifications



Cet onglet affiche la liste des activités des utilisateurs liées à l'évaluation.

Le tableau Journal des modifications présente une liste de comptes contenant les données suivantes :

- Date : date de l'activité.
- Utilisateur : utilisateur qui a effectué l'action.
- Action : action qui s'est produite, telle qu'une évaluation en cours de création.
- Type : type d'objet qui a changé, par exemple une évaluation.
- Ressource : ressource affectée par la modification, telle que le cadre à partir duquel l'évaluation a été créée.

Vérification des contrôles dans le cadre d'une évaluation

Les contrôles d'Audit Manager vous aident à respecter les normes et réglementations de conformité communes et uniques dans le cadre de vos audits. Vous pouvez ouvrir et vérifier les contrôles de votre évaluation Audit Manager à tout moment.

Pour ouvrir une page de résumé des contrôles

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations, puis sélectionnez le nom d'une évaluation pour l'ouvrir.
3. Sur la page d'évaluation, choisissez l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'au tableau des Ensembles de contrôles, puis choisissez le nom d'un contrôle pour l'ouvrir.

Lorsque vous ouvrez un contrôle, une page de résumé contenant plusieurs sections s'affiche. Les sections de cette page et leur contenu sont décrits dans les sections suivantes.

Sections de la page de contrôle

- Détails du contrôle
- Mettre à jour le statut du contrôle
- Onglet Dossiers de preuves
- Onglet Source de données
- Onglet des commentaires
- Onglet Journal des modifications

Détails du contrôle

La section Détails du contrôle fournit une présentation du contrôle.

Il contient les informations suivantes :

1. Nom du contrôle : nom donné à ce contrôle.
2. Description du contrôle : description fournie pour ce contrôle.
3. Informations de test : procédures de test recommandées pour ce contrôle.
4. Plan d'action : actions recommandées à effectuer si le contrôle n'est pas probant.

Mettre à jour le statut du contrôle

Dans la section Mettre à jour le statut du contrôle de la page, vous pouvez consulter et mettre à jour le statut du contrôle d'évaluation.

Les états disponibles sont les suivants :

- En cours de vérification : indique que ce contrôle n'a pas encore été vérifié. Des preuves sont toujours en cours de collecte pour ce contrôle, et vous pouvez charger des preuves manuelles. Il s'agit du statut par défaut.
- Vérifié : indique que les preuves de ce contrôle sont vérifiées. Les preuves sont toujours en cours de collecte et vous pouvez charger des preuves manuelles.
- Inactif : indique que la collecte automatique de preuves est interrompue pour ce contrôle. Vous ne pouvez plus télécharger de preuves manuelles.

> **Note**
>
> La modification du statut d'un contrôle en Vérifié est définitive. Une fois que vous avez défini le statut d'un contrôle sur Vérifié, vous ne pouvez plus modifier le statut de ce contrôle ni revenir à un statut précédent.

Onglet Dossiers de preuves

L'onglet Dossiers de preuves répertorie les preuves automatiquement collectées pour ce contrôle. Il est organisé en dossiers sur une base quotidienne.

Le tableau Dossiers de preuves présente une liste de dossiers contenant les données suivantes :

- Dossier de preuves : nom du dossier de preuves. Le nom est basé sur la date à laquelle les preuves ont été collectées ou ajoutées manuellement.
- Contrôle de conformité : nombre de problèmes détectés dans le dossier de preuves. Ce nombre représente le nombre total de problèmes de sécurité qui ont été signalés directement depuis AWS Security Hub, AWS Config, ou depuis les deux. Si l'indication Sans objet s'affiche, cela signifie soit que ni AWS Security Hub ni AWS Config n'est activé, soit que les preuves proviennent d'un autre type de source de données.
- Total des preuves : nombre total d'éléments de preuve contenus dans le dossier.
- Sélection du rapport d'évaluation : nombre d'éléments de preuve liés à ce contrôle qui ont été inclus dans le rapport d'évaluation.

Dans l'onglet Dossiers de preuves, vous pouvez effectuer les actions suivantes :

- Passez en revue les preuves individuelles : choisissez un dossier de preuves pour l'ouvrir. Sur la page de résumé du dossier de preuves, vous pouvez ensuite choisir les preuves individuelles que vous souhaitez examiner.
- Ajouter des preuves manuelles : pour de plus amples informations, veuillez consulter Ajouter des preuves manuelles dans AWS Audit Manager.
- Ajouter des preuves à un rapport d'évaluation : pour plus d'informations, veuillez consulter Génération de rapports d'évaluation.

Onglet Source de données

Cet onglet affiche des informations sur les sources de données du contrôle. Il contient les informations suivantes :

- Nom de la source de données : concerne uniquement les contrôles personnalisés. Il fait référence au nom descriptif que vous avez attribué à chaque source de données. Vous pouvez utiliser ce nom pour faire la distinction entre plusieurs sources de données relevant du même type de source de données
- Type de source de données : indique d'où proviennent les données probantes.
  - Si Audit Manager collecte les preuves, la source de données peut être de quatre types : AWS Security Hub, AWS Config, AWS CloudTrail ou AWS appels d'API.
  - Si vous chargez vos propres preuves, le type de source de données est Manuel. Une description indique si la preuve manuelle requise est un Chargement de fichier ou une Réponse sous forme de texte.
- Mappage : il s'agit de l'attribut de mappage utilisé pour identifier et récupérer les données d'une source de données automatisée.
  - Si le type de source de données est AWS Config, le mappage est le nom d'une règle AWS Config spécifique (par exemple, `EC2_INSTANCE_MANAGED_BY_SSM`). Audit Manager utilise ce mappage pour signaler le résultat de cette vérification des règles directement à partir de AWS Config.
  - Si le type de source de données est AWS Security Hub, le mappage est le nom d'un contrôle Security Hub spécifique (par exemple, `1.1 – Avoid the use of the "root" account`). Audit Manager utilise ce mappage pour signaler le résultat de ce contrôle de sécurité directement à partir du Security Hub.
  - Si le type de source de données est un appel d'API AWS, le mappage est le nom d'un appel d'API spécifique (par exemple, `ec2_DescribeSecurityGroups`). Audit Manager utilise ce mappage pour collecter la réponse de l'API.
  - Si le type de source de données est AWS CloudTrail, le mappage est le nom d'un événement CloudTrail spécifique (par exemple, `CreateAccessKey`). Audit Manager utilise ce mappage pour collecter l'activité utilisateur associée à partir de vos journaux CloudTrail.
- Fréquence : fréquence de collecte de preuves à partir de cette source de données. La fréquence varie en fonction de la source de données. Pour plus d'informations, choisissez la valeur dans la colonne ou consultez Fréquence de collecte des preuves.

Onglet des commentaires

Dans l'onglet Commentaires, vous pouvez ajouter un commentaire concernant le contrôle et ses preuves. Il affiche également une liste de commentaires précédents.

Sous Envoyer des commentaires, vous pouvez ajouter des commentaires pour un contrôle en saisissant du texte, puis en choisissant Soumettre les commentaires.

Sous Commentaires précédents, vous pouvez consulter la liste des commentaires précédents ainsi que la date à laquelle chaque commentaire a été publié et le nom d'utilisateur associé.

Onglet Journal des modifications

L'onglet Journal des modifications affiche une liste des activités des utilisateurs liées au contrôle. Les mêmes informations sont disponibles lorsque la piste d'audit se connecte dans AWS CloudTrail. Grâce à l'activité des utilisateurs capturée directement dans Audit Manager, vous pouvez facilement consulter une piste d'audit de l'activité d'un contrôle donné.

Sous Journal des modifications, un tableau affiche les colonnes de données suivantes :

- Date : date et heure de l'activité, exprimées en heure UTC (Temps universel coordonné).
- Utilisateur : utilisateur ou rôle qui a effectué l'activité.
- Action : description de l'activité.
- Type : attribut associé qui décrit plus en détail l'activité.
- Ressource : ressource associée, le cas échéant.

Audit Manager suit les activités des utilisateurs suivantes dans les journaux des modifications :

- Création d'une évaluation
- Modification d'une évaluation
- Complétion d'une évaluation
- Suppression d'une évaluation
- Délégation d'un ensemble de contrôles à des fins d'examen
- Soumission d'un ensemble de contrôles vérifié au responsable de l'audit
- Chargement de preuves manuelles
- Mise à jour du statut d'un contrôle
- Génération de rapports d'évaluation

Examen des preuves dans le cadre d'une évaluation

Chaque évaluation active dans Audit Manager recueille automatiquement des preuves à partir de diverses sources de données. Pour de plus amples informations, veuillez consulter De quelle façon AWS Audit Manager recueille les preuves. Vous pouvez ouvrir et vérifier les preuves pour les contrôles de votre évaluation à tout moment.

Pour ouvrir des preuves en vue d'un contrôle

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations, puis sélectionnez le nom d'une évaluation pour l'ouvrir.
3. Sur la page d'évaluation, choisissez l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'au tableau Contrôles, puis choisissez le nom d'un contrôle pour l'ouvrir.
4. Sur la page détaillée du contrôle, choisissez l'onglet Dossiers de preuves. Une liste des dossiers contenant les preuves de ce contrôle est affichée dans Dossiers de preuves. Ces dossiers sont organisés et nommés en fonction de la date à laquelle les preuves contenues dans ce dossier ont été collectées.
5. Sélectionnez le nom d'un dossier d'éléments probants pour l'ouvrir.

À partir de là, vous pouvez désormais consulter les dossiers de preuves relatifs à ce contrôle, et effectuer une analyse plus approfondie pour examiner les éléments de preuve individuels selon les besoins.

Rubriques

- Examen des dossiers de preuves
- Examen des preuves individuelles

Examen des dossiers de preuves

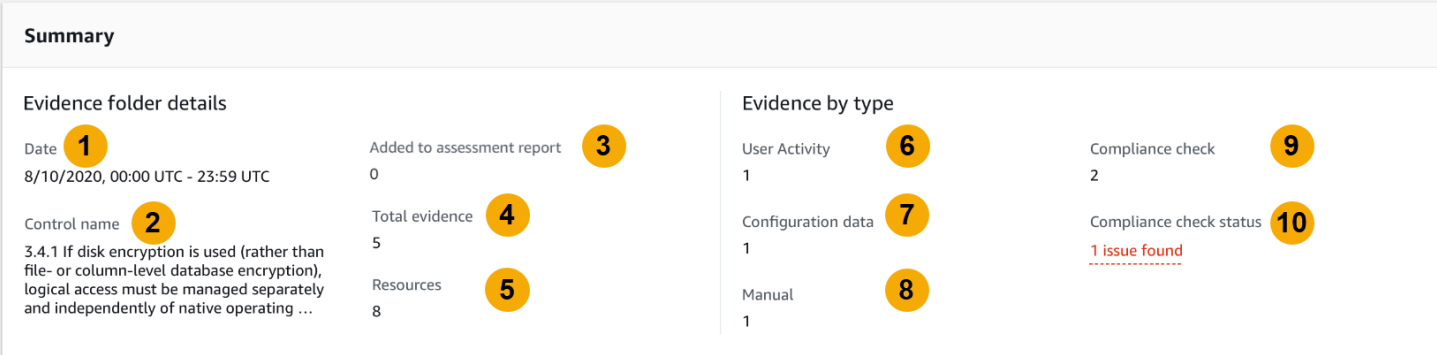
Lorsque vous ouvrez un dossier de preuves, vous voyez une page récapitulative du dossier de preuves qui contient deux sections : une section Résumé et un tableau de Preuves. Les sections et leur contenu sont décrits comme suit.

- Résumé du dossier de preuves

- Tableau des preuves

Résumé du dossier de preuves

La section Résumé de la page fournit un aperçu général des preuves contenues dans le dossier des preuves.



Il contient les informations suivantes :

1. Date : date et heure de création du dossier de preuves, exprimées en heure UTC (Temps universel coordonné).
2. Nom du contrôle : nom du contrôle associé à ce dossier de preuves.
3. Ajouté au rapport d'évaluation : nombre d'éléments de preuve liés à ce contrôle qui ont été sélectionnés manuellement pour être inclus dans le rapport d'évaluation.
4. Total des preuves : nombre total d'éléments de preuve contenus dans le dossier des preuves.
5. Ressources : nombre total de ressources AWS évaluées lors de la génération des preuves contenues dans ce dossier.
6. Activité des utilisateurs : nombre d'éléments de preuve relevant de la catégorie Activité des utilisateurs. Ces preuves sont collectées à partir de journaux AWS CloudTrail.
7. Données de configuration : nombre d'éléments de preuve relevant de la catégorie Données de configuration. Ces preuves sont collectées à partir d'instantanés de configuration d'autres ressources Services AWS telles qu'Amazon EC2, Amazon S3 ou IAM.
8. Manuel : nombre d'éléments de preuve relevant de la catégorie Manuel. Ces preuves sont chargées manuellement.
9. Contrôle de conformité : nombre d'éléments de preuve relevant de la catégorie Contrôle de conformité. Ces preuves sont recueillies auprès de AWS Config ou AWS Security Hub.

10. Statut du contrôle de conformité : nombre total de problèmes signalés directement par AWS Security Hub,AWS Config, ou par les deux.

> **Tip**
>
> Pour plus d'informations sur les différents types de preuves (activité des utilisateurs, données de configuration, contrôle de conformité et manuel), veuillez consulter la section Preuves.

Tableau des preuves

Le tableau des Preuves répertorie les éléments de preuve individuels contenus dans le dossier de preuves.

Il contient les informations suivantes :

1. Heure : précise le moment où les preuves ont été collectées et sert également de nom aux preuves. L'heure est représentée au format UTC (temps universel coordonné). Le choix d'une heure dans cette colonne ouvre une page détaillée des preuves. Cette page est décrite dans la section suivante.
2. Preuve par type : catégorie de preuve.
   - Les preuves du Contrôle de conformité sont collectées auprès de AWS Config ou AWS Security Hub.
   - Les preuves de l'activité des utilisateurs sont collectées à partir des journaux AWS CloudTrail.
   - Les preuves des données de configuration sont collectées à partir de captures d'écran d'autres services tels qu'Amazon EC2, Amazon S3 ou IAM.
   - Les preuves manuelles sont des preuves que vous chargez manuellement.
3. Contrôle de conformité : le statut d'évaluation des preuves relevant de la catégorie du contrôle de conformité.
   - Pour les preuves collectées auprès de AWS Security Hub, un résultat de réussite ou d'échec est signalé directement depuis AWS Security Hub.
   - Pour les preuves collectées auprès de AWS Config, un résultat conforme ou non conforme est signalé directement depuis AWS Config.
   - Si l'indication Sans objet s'affiche, cela signifie soit que ni AWS Security Hub ni AWS Config n'est activé, soit que les preuves proviennent d'un autre type de source de données.

4. Source de données : source de données à partir de laquelle les preuves sont collectées.
5. Nom de l'événement :nom de l'événement inclus dans les preuves.
6. Ressources : nombre de ressources évaluées pour générer les preuves.
7. Sélection du rapport d'évaluation : indique si ces preuves ont été sélectionnées manuellement pour être incluses dans le rapport d'évaluation.
   - Pour inclure des preuves, sélectionnez les preuves et choisissez Ajouter au rapport d'évaluation.
   - Pour exclure des preuves, sélectionnez-les et choisissez Supprimer du rapport d'évaluation.

Pour charger des preuves manuelles dans le dossier des preuves, choisissez Charger des preuves manuelles, entrez l'URI S3 des preuves, puis choisissez Charger. Pour de plus amples informations, veuillez consulter Charger des preuves manuelles dans AWS Audit Manager.

Pour voir les détails d'un élément de preuve individuel, choisissez le nom de la preuve en hyperlien dans la colonne Heure. Cette action ouvre une page détaillée des preuves, décrite dans la section suivante.

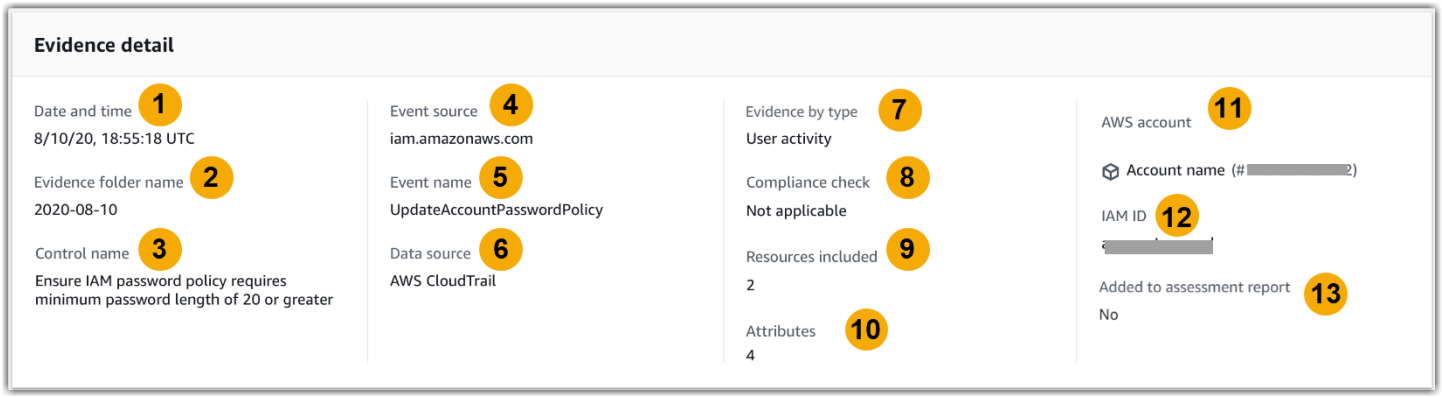
Examen des preuves individuelles

Lorsque vous ouvrez un élément de preuve individuel, vous voyez une page détaillée des preuves qui contient trois sections : la section Détails des preuves, le tableau des Attributs et le tableau des Ressources incluses. Les sections et leur contenu sont décrits comme suit.

- Détail des preuves
- Attributs
- Ressources incluses

Détail des preuves

La section Détail des preuves de la page affiche un aperçu des preuves.



Il contient les informations suivantes :

1. Date et heure : date et heure de collecte des preuves, exprimées en heure UTC (Temps universel coordonné).
2. Nom du dossier de preuves : nom du dossier de preuves qui contient les preuves.
3. Nom du contrôle : nom du contrôle associé à ce dossier de preuves.
4. Source de l'événement : nom de la ressource qui a créé l'événement de preuve.
5. Nom de l'événement : nom de l'événement de preuve.
6. Source de données : source de données à partir de laquelle les preuves ont été collectées.
7. Preuve par type : type de preuve.
   - Les preuves du Contrôle de conformité sont collectées auprès de AWS Config ou AWS Security Hub.
   - Les preuves de l'activité des utilisateurs sont collectées à partir des journaux AWS CloudTrail.
   - Les preuves des données de configuration sont collectées à partir d'instantanés d'autres Services AWS tels qu'Amazon EC2, Amazon S3 ou IAM.
   - Les preuves manuelles sont des preuves que vous chargez manuellement.
8. Contrôle de conformité : le statut d'évaluation des preuves relevant de la catégorie du contrôle de conformité.
   - Pour les preuves collectées auprès de AWS Security Hub, un résultat de réussite ou d'échec est signalé directement depuis AWS Security Hub.
   - Pour les preuves collectées auprès de AWS Config, un résultat conforme ou non conforme est signalé directement depuis AWS Config.
   - Si l'indication Sans objet s'affiche, cela signifie soit que ni AWS Security Hub ni AWS Config n'est activé, soit que les preuves proviennent d'un autre type de source de données.
9. Ressources incluses : le nombre de ressources évaluées pour générer les preuves.

10. Attributs : nombre total d'attributs utilisés par l'événement dans les preuves.
11. Compte AWS : le Compte AWS d'où les preuves ont été recueillies.
12. ID IAM : l'utilisateur ou le rôle concerné, le cas échéant.
13. Ajouté au rapport d'évaluation : indique si vous avez choisi d'inclure les preuves dans le rapport d'évaluation.

Attributs

Le tableau Attributs affiche les noms et les valeurs utilisés par l'événement dans ces preuves. Il contient les informations suivantes :

- Nom de l'attribut : exigence relative aux preuves, telles que AllowUsersToChangePassword.
- Valeur : valeur de l'attribut, telle que vrai ou faux.

Ressources incluses

Le tableau Ressources incluses affiche la liste des ressources évaluées pour générer ces preuves. Il inclut un ou plusieurs des champs suivants :

- ARN : l'Amazon Resource Name (ARN) de la ressource. Un ARN peut ne pas être disponible pour tous les types de preuves.
- Valeur : valeur de cette ressource, le cas échéant.
- JSON : le lien permettant d'afficher le fichier JSON pour cette ressource.

Ajouter des preuves manuelles dans AWS Audit Manager

Audit Manager peut collecter automatiquement des preuves pour de nombreux contrôles. Cependant, certains contrôles nécessitent que vous ajoutiez manuellement vos propres preuves.

Considérez les exemples suivants :

- Certains contrôles concernent la fourniture d'enregistrements physiques (tels que des signatures) ou des événements qui ne sont pas générés dans le cloud (tels que des observations et des entretiens). Dans ces cas, vous pouvez charger manuellement des fichiers à titre de preuve. Par exemple, si un contrôle nécessite des informations sur votre structure organisationnelle, vous pouvez charger une copie de l'organigramme de votre entreprise à titre de preuve manuelle.

- Certains contrôles constituent une question d'évaluation des risques liés aux fournisseurs. Une question d'évaluation des risques peut nécessiter de la documentation à titre de preuve (comme un organigramme). Ou bien, il se peut qu'une simple réponse textuelle (telle qu'une liste des titres de poste) soit nécessaire. Dans ce dernier cas, vous pouvez répondre à la question et enregistrer votre réponse sous forme de preuve manuelle.

Vous pouvez également utiliser la fonctionnalité de chargement manuel pour gérer les preuves provenant de plusieurs environnements. Si votre entreprise utilise un modèle de cloud hybride ou multicloud, vous pouvez charger des preuves depuis votre environnement sur site, un environnement hébergé dans le cloud ou vos applications SaaS. Cela vous permet d'organiser vos preuves (quelle que soit leur provenance) en les stockant dans la structure d'une évaluation d'Audit Manager, où chaque élément probant est associé à un contrôle spécifique.

Pour en savoir plus sur les différents types de preuves dans Audit Manager, veuillez consulter la section Preuves dans la section de ce guide consacrée aux concepts et à la terminologie.

Comment ajouter des preuves manuelles

Vous pouvez utiliser l'une des méthodes suivantes pour ajouter vos propres preuves manuelles à un contrôle d'évaluation.

Gardez à l'esprit les points suivants :

- Vous ne pouvez utiliser qu'une seule méthode à la fois pour ajouter des preuves manuelles.
- La taille maximale prise en charge pour un seul fichier de preuve manuel est de 100 Mo.
- Les Formats de fichier pris en charge pour les preuves manuelles sont listés plus bas sur cette page.
- Chaque Compte AWS ne peut charger manuellement que 100 fichiers de preuves maximum dans un contrôle par jour. Le dépassement de ce quota quotidien entraîne l'échec de tout chargement manuel supplémentaire pour le contrôle en question. Si vous devez charger une grande quantité de preuves manuelles dans un seul contrôle, chargez-les par lots sur plusieurs jours.
- Lorsqu'un contrôle est inactif, vous ne pouvez pas charger de preuves manuelles pour ce contrôle. Pour ajouter des preuves manuelles, vous devez d'abord faire passer le statut du contrôle sur en cours de vérification ou vérifié. Pour obtenir des instructions, veuillez consulter Mettre à jour le statut du contrôle.

Importer un fichier à partir d'Amazon S3

Procédez comme suit pour importer des preuves manuelles à partir d'un compartiment S3.

AWS console

Importation d'un fichier à partir de S3 (console)

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations, puis sélectionnez le nom d'une évaluation pour l'ouvrir.
3. Choisissez l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'à Ensembles de contrôles, puis choisissez le nom d'un contrôle pour l'ouvrir.
4. Dans l'onglet Dossiers de preuves, choisissez Ajouter des preuves manuelles, puis choisissez Importer un fichier depuis S3.
   - Vous pouvez également choisir un nom de dossier de preuves dans l'onglet Dossiers de preuves pour consulter le résumé du dossier de preuves, puis choisir Ajouter des preuves manuelles, Importer un fichier depuis S3.
5. Sur la page suivante, saisissez l'URI S3 des preuves. Vous pouvez trouver l'URI S3 en accédant à l'objet dans la console Amazon S3 et en choisissant Copy S3 URI.
6. Sélectionnez Charger.

AWS CLI

Dans la procédure suivante, remplacez le *texte de l'espace réservé* par vos propres informations.

Importation d'un fichier à partir de S3 (CLI)

1. Exécutez la commande `list-assessments` pour afficher la liste de vos évaluations.

```
aws auditmanager list-assessments
```

   Dans la réponse, recherchez l'évaluation dans laquelle vous souhaitez charger des preuves et notez l'identifiant de l'évaluation.

2. Exécutez la commande `get-assessment` et spécifiez l'ID d'évaluation indiqué à la première étape.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

   Dans la réponse, recherchez l'ensemble de contrôles et le contrôle vers lesquels vous souhaitez charger des preuves, et notez leurs identifiants.

3. Exécutez la commande `batch-import-evidence-to-assessment-control` avec les paramètres suivants :

   - `--assessment-id`— Utilisez l'identifiant d'évaluation indiqué à l'étape 1.
   - `--control-set-id`— Utilisez l'identifiant de l'ensemble de contrôles indiqué à l'étape 2.
   - `--control-id`— Utilisez l'identifiant de contrôle indiqué à l'étape 2.
   - `--manual-evidence`— Utilisez `s3ResourcePath` comme type de preuve manuel et spécifiez l'URI S3 de la preuve. Vous pouvez trouver l'URI S3 en accédant à l'objet dans la console Amazon S3 et en choisissant Copy S3 URI.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence s3ResourcePath=s3://
example-bucket/example-file.extension
```

Audit Manager API

Importation d'un fichier à partir de S3 (API)

1. Appelez l'opération `ListAssessments` pour obtenir la liste de vos évaluations. Dans la réponse, recherchez l'évaluation dans laquelle vous souhaitez charger des preuves et notez l'identifiant de l'évaluation.
2. Appelez l'opération `GetAssessment` et spécifiez l'identifiant d'évaluation indiqué à la première étape. Dans la réponse, recherchez l'ensemble de contrôles et le contrôle vers lesquels vous souhaitez charger des preuves, et notez leurs identifiants.
3. Appelez l'opération `BatchImportEvidenceToAssessmentControl` avec les paramètres suivants :

- `assessmentId`— Utilisez l'identifiant d'évaluation indiqué à l'étape 1.
- `controlSetId`— Utilisez l'identifiant de l'ensemble de contrôles indiqué à l'étape 2.
- `controlId`— Utilisez l'identifiant de contrôle indiqué à l'étape 2.
- `manualEvidence`— Utilisez `s3ResourcePath` comme type de preuve manuel et spécifiez l'URI S3 de la preuve. Vous pouvez trouver l'URI S3 en accédant à l'objet dans la console Amazon S3 et en choisissant Copy S3 URI.

Pour plus d'informations, choisissez l'un des liens précédents dans le Guide de référence de l'API AWS Audit Manager. Il inclut des informations sur l'utilisation du fonctionnement et des paramètres dans l'un des SDK AWS spécifiques au langage.

Charger un fichier à partir de votre navigateur

Suivez ces étapes pour charger des preuves manuellement depuis votre navigateur.

AWS console

Pour charger un fichier depuis votre navigateur (console)

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations, puis sélectionnez le nom d'une évaluation pour l'ouvrir.
3. Dans l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'à Ensembles de contrôles, puis choisissez le nom d'un contrôle pour l'ouvrir.

   À partir de là, vous pouvez charger un fichier de trois manières :

   - (Option 1) Dans le bandeau de notification bleu, choisissez Charger des preuves manuelles.
   - (Option 2) Dans l'onglet Dossiers de preuves, choisissez Ajouter des preuves manuelles, puis choisissez Charger le fichier depuis le navigateur.
   - (Option 3) Choisissez un nom de dossier de preuves pour consulter un résumé de ce dossier, choisissez Ajouter des preuves manuelles, puis choisissez Charger le fichier depuis le navigateur.
4. Choisissez le dossier que vous souhaitez charger.

5. Sélectionnez Charger.

AWS CLI

Dans la procédure suivante, remplacez le *texte de l'espace réservé* par vos propres informations.

Pour charger un fichier depuis votre navigateur (CLI)

1. Exécutez la commande `list-assessments` pour afficher la liste de vos évaluations.

```
aws auditmanager list-assessments
```

   Dans la réponse, recherchez l'évaluation dans laquelle vous souhaitez charger des preuves et notez l'identifiant de l'évaluation.

2. Exécutez la commande `get-assessment` et spécifiez l'ID d'évaluation indiqué à la première étape.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

   Dans la réponse, recherchez l'ensemble de contrôles et le contrôle vers lesquels vous souhaitez charger des preuves, et notez leurs identifiants.

3. Exécutez la commande`get-evidence-file-upload-url` et spécifiez le fichier que vous voulez charger.

```
aws auditmanager get-evidence-file-upload-url --file-name fileName.extension
```

   Dans la réponse, prenez note de l'URL présignée et du `evidenceFileName`.

4. Utilisez l'URL présignée de la troisième étape pour charger le fichier depuis votre navigateur. Cette action charge votre fichier sur Amazon S3, où il est enregistré en tant qu'objet pouvant être joint à un contrôle d'évaluation. Dans l'étape suivante, vous allez référencer l'objet nouvellement créé à l'aide du paramètre `evidenceFileName`.

> **Note**
>
> Lorsque vous chargez un fichier à l'aide d'une URL présignée, Audit Manager protège et stocke vos données en utilisant le chiffrement côté serveur avec AWS Key Management Service. À cette fin, vous devez utiliser l'en-tête `x-amz-server-side-encryption` de votre demande lorsque vous utilisez l'URL présignée pour charger votre fichier.
>
> Si vous utilisez un client géré dans les paramètres AWS KMS key de votre Audit Manager Chiffrement des données, assurez-vous d'inclure également l'en-tête `x-amz-server-side-encryption-aws-kms-key-id` dans votre demande. Si l'en-tête `x-amz-server-side-encryption-aws-kms-key-id` n'est pas présent dans la demande, Amazon S3 suppose que vous souhaitez utiliser la Clé gérée par AWS.
>
> Pour plus d'informations, veuillez consulter la section Protection des données à l'aide du chiffrement côté serveur avec les AWS Key Management Service clés KMS (SSE-KMS) dans le Guide de l'utilisateur Amazon Simple Storage Service.

5. Exécutez la commande `batch-import-evidence-to-assessment-control` avec les paramètres suivants :

   - `--assessment-id`— Utilisez l'identifiant d'évaluation indiqué à l'étape 1.
   - `--control-set-id`— Utilisez l'identifiant de l'ensemble de contrôles indiqué à l'étape 2.
   - `--control-id`— Utilisez l'identifiant de contrôle indiqué à l'étape 2.
   - `--manual-evidence`— Utilisez `evidenceFileName` comme type de preuve manuel et spécifiez le nom du fichier de preuves à l'étape 3.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet
 --control-id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence
 evidenceFileName=fileName.extension
```

Audit Manager API

Pour charger un fichier depuis votre navigateur (API)

1. Appelez l'opération `ListAssessments`. Dans la réponse, recherchez l'évaluation dans laquelle vous souhaitez charger des preuves et notez l'identifiant de l'évaluation.
2. Appelez l'opération `GetAssessment` et spécifiez la `assessmentId` à partir de la première étape. Dans la réponse, recherchez l'ensemble de contrôles et le contrôle vers lesquels vous souhaitez charger des preuves, et notez leurs identifiants.
3. Appelez l'opération `GetEvidenceFileUploadUrl` et précisez le fichier `fileName` que vous souhaitez charger. Dans la réponse, prenez note de l'URL présignée et du `evidenceFileName`.
4. Utilisez l'URL présignée de la troisième étape pour charger le fichier depuis votre navigateur. Cette action charge votre fichier sur Amazon S3, où il est enregistré en tant qu'objet pouvant être joint à un contrôle d'évaluation. Dans l'étape suivante, vous allez référencer l'objet nouvellement créé à l'aide du paramètre `evidenceFileName`.

   > **Note**
   >
   > Lorsque vous chargez un fichier à l'aide d'une URL présignée, Audit Manager protège et stocke vos données en utilisant le chiffrement côté serveur avec AWS Key Management Service. À cette fin, vous devez utiliser l'en-tête `x-amz-server-side-encryption` de votre demande lorsque vous utilisez l'URL présignée pour charger votre fichier.
   >
   > Si vous utilisez un client géré dans les paramètres AWS KMS key de votre Audit Manager Chiffrement des données, assurez-vous d'inclure également l'en-tête `x-amz-server-side-encryption-aws-kms-key-id` dans votre demande. Si l'en-tête `x-amz-server-side-encryption-aws-kms-key-id` n'est pas présent dans la demande, Amazon S3 suppose que vous souhaitez utiliser la Clé gérée par AWS.
   >
   > Pour plus d'informations, veuillez consulter la section Protection des données à l'aide du chiffrement côté serveur avec les AWS Key Management Service clés KMS (SSE-KMS) dans le Guide de l'utilisateur Amazon Simple Storage Service.

5. Appelez l'opération `BatchImportEvidenceToAssessmentControl` avec les paramètres suivants :

- `assessmentId`— Utilisez l'identifiant d'évaluation indiqué à l'étape 1.
- `controlSetId`— Utilisez l'identifiant de l'ensemble de contrôles indiqué à l'étape 2.
- `controlId`— Utilisez l'identifiant de contrôle indiqué à l'étape 2.
- `manualEvidence`— Utilisez `evidenceFileName` comme type de preuve manuel et spécifiez le nom du fichier de preuves à l'étape 3.

Pour plus d'informations, choisissez l'un des liens précédents dans le Guide de référence de l'API AWS Audit Manager. Il inclut des informations sur l'utilisation du fonctionnement et des paramètres dans l'un des SDK AWS spécifiques au langage.

Entrez une réponse textuelle

Suivez ces étapes pour saisir une réponse à une question d'évaluation des risques et enregistrer votre réponse sous forme de preuve manuelle.

AWS console

Pour saisir une réponse textuelle (console)

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations, puis sélectionnez le nom d'une évaluation pour l'ouvrir.
3. Choisissez l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'à Ensembles de contrôles, puis choisissez le nom d'un contrôle pour l'ouvrir.

   À partir de là, vous pouvez saisir une réponse textuelle de trois manières :

   - (Option 1) Dans le bandeau de notification bleu, choisissez Saisir la réponse.
   - (Option 2) Dans l'onglet Dossiers de preuves, choisissez Ajouter des preuves manuelles, puis choisissez Saisir une réponse textuelle.
   - (Option 3) Choisissez un dossier de preuves pour consulter un résumé de ce dossier, choisissez Ajouter des preuves manuelles, puis choisissez Saisir une réponse textuelle.
4. Dans la fenêtre contextuelle qui apparaît, saisissez votre réponse en texte brut.
5. Choisissez Confirmer.

AWS CLI

Dans la procédure suivante, remplacez le *texte de l'espace réservé* par vos propres informations.

Pour saisir une réponse textuelle (CLI)

1. Exécutez la commande `list-assessments`.

```
aws auditmanager list-assessments
```

   Dans la réponse, recherchez l'évaluation dans laquelle vous souhaitez charger des preuves et notez l'identifiant de l'évaluation.

2. Exécutez la commande `get-assessment` et spécifiez l'ID d'évaluation indiqué à la première étape.

```
aws auditmanager get-assessment --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p
```

   Dans la réponse, recherchez l'ensemble de contrôles et le contrôle vers lesquels vous souhaitez charger des preuves, et notez leurs identifiants.

3. Exécutez la commande `batch-import-evidence-to-assessment-control` avec les paramètres suivants :

   - `--assessment-id`— Utilisez l'identifiant d'évaluation indiqué à l'étape 1.
   - `--control-set-id`— Utilisez l'identifiant de l'ensemble de contrôles indiqué à l'étape 2.
   - `--control-id`— Utilisez l'identifiant de contrôle indiqué à l'étape 2.
   - `--manual-evidence`— `textResponse` Utilisez-le comme type de preuve manuelle et entrez le texte que vous souhaitez enregistrer en tant que preuve manuelle.

```
aws auditmanager batch-import-evidence-to-assessment-control --assessment-
id 1a2b3c4d-5e6f-7g8h-9i0j-0k1l2m3n4o5p --control-set-id ControlSet --control-
id a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6 --manual-evidence textResponse="enter
 text here"
```

Audit Manager API

Pour saisir une réponse textuelle (API)

1. Appelez l'opération `ListAssessments`. Dans la réponse, recherchez l'évaluation dans laquelle vous souhaitez charger des preuves et notez l'identifiant de l'évaluation.
2. Appelez l'opération `GetAssessment` et spécifiez la `assessmentId` à partir de la première étape. Dans la réponse, recherchez l'ensemble de contrôles et le contrôle vers lesquels vous souhaitez charger des preuves, et notez leurs identifiants.
3. Appelez l'opération `BatchImportEvidenceToAssessmentControl` avec les paramètres suivants :
   - `assessmentId`— Utilisez l'identifiant d'évaluation indiqué à l'étape 1.
   - `controlSetId`— Utilisez l'identifiant de l'ensemble de contrôles indiqué à l'étape 2.
   - `controlId`— Utilisez l'identifiant de contrôle indiqué à l'étape 2.
   - `manualEvidence`— `textResponse` Utilisez-le comme type de preuve manuelle et entrez le texte que vous souhaitez enregistrer en tant que preuve manuelle.

Pour plus d'informations, choisissez l'un des liens précédents dans le Guide de référence de l'API AWS Audit Manager. Il inclut des informations sur l'utilisation du fonctionnement et des paramètres dans l'un des SDK AWS spécifiques au langage.

Formats de fichier pris en charge pour les preuves manuelles

Le tableau ci-dessous répertorie et décrit les types de fichiers que vous pouvez charger à titre de preuve manuelle. Pour chaque type de fichier, le tableau répertorie également les extensions de fichier prises en charge.

Type de fichier	Description	Extensions de fichier prises en charge
Compression ou archivage	Archives compressées GNU et archives compressées ZIP	`.gz`, `.zip`
Document	Fichiers de documents courants tels que les PDF	`.doc`, `.docx`, `.pdf`, `.ppt`, `.pptx`, `.xls`, `.xlsx`

Type de fichier	Description	Extensions de fichier prises en charge
	et les fichiers Microsoft Office	
Image	Fichiers d'images et de graphiques	`.jpeg`, `.jpg`, `.png`, `.svg`
Texte	Autres fichiers texte non binaires, tels que les documents en texte brut et les fichiers de langage de balisage	`.cer`, `.csv`, `.html`, `.jmx`, `.json`, `.md`, `.out`, `.rtf`, `.txt`, `.xml`, `.yaml`, `.yml`

Génération de rapports d'évaluation

Un rapport d'évaluation résume votre évaluation et fournit des liens vers un ensemble organisé de dossiers contenant des preuves connexes. Pour de plus amples informations, veuillez consulter Rapports d'évaluation.

Vous pouvez choisir les preuves que vous souhaitez inclure dans votre rapport d'évaluation avant de générer le rapport d'évaluation. Les preuves récemment recueillies ne sont pas automatiquement incluses dans un rapport d'évaluation.

Tâches

- Ajouter des preuves à un rapport d'évaluation
- Supprimer des preuves d'un rapport d'évaluation
- Génération de rapports d'évaluation
- Que puis-je faire ensuite ?

Ajouter des preuves à un rapport d'évaluation

Avant de pouvoir générer un rapport d'évaluation, vous devez ajouter au moins un élément de preuve à votre rapport d'évaluation. Vous pouvez soit ajouter un dossier de preuves complet, soit ajouter des éléments de preuve individuels à partir d'un dossier.

Ajouter des preuves à un rapport d'évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations, puis sélectionnez le nom d'une évaluation pour l'ouvrir.
3. Dans l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'au tableau des Ensembles de contrôles et choisissez le nom d'un contrôle pour l'ouvrir.
4. Choisissez comment ajouter des preuves à votre rapport d'évaluation.

   a. Pour ajouter un dossier de preuves complet, faites défiler l'écran vers le bas jusqu'à Dossiers de preuves, sélectionnez le dossier que vous souhaitez ajouter, puis choisissez Ajouter au rapport d'évaluation.

      - Si le dossier que vous recherchez ne s'affiche pas, définissez le filtre déroulant sur Toutes les dates. Dans le cas contraire, les dossiers des sept derniers jours s'afficheront par défaut.
      - Si Ajouter au rapport d'évaluation est grisé, le dossier de preuves a déjà été ajouté au rapport d'évaluation.

   b. Pour ajouter des preuves spécifiques, choisissez un dossier de preuves pour ouvrir son contenu. Sélectionnez un ou plusieurs éléments dans la liste, puis choisissez Ajouter au rapport d'évaluation.

      - Si Ajouter au rapport d'évaluation est grisé, assurez-vous d'avoir coché la case à côté des preuves, puis réessayez.

5. Une fois que vous avez ajouté les preuves au rapport d'évaluation, un bandeau vert de réussite apparaît. Choisissez Afficher les preuves dans le rapport d'évaluation pour voir les preuves qui seront incluses dans votre rapport d'évaluation.

   - Vous pouvez également consulter les preuves qui seront incluses dans votre rapport d'évaluation en revenant à votre évaluation et en choisissant l'onglet de sélection du rapport d'évaluation.

Supprimer des preuves d'un rapport d'évaluation

Si vous devez supprimer des preuves d'un rapport d'évaluation, procédez comme suit. Vous pouvez soit supprimer un dossier de preuves complet, soit supprimer des éléments de preuve individuels à partir d'un dossier.

Pour supprimer des preuves d'un rapport d'évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations, puis sélectionnez le nom d'une évaluation pour l'ouvrir.
3. Dans l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'au tableau des Ensembles de contrôles et choisissez le nom d'un contrôle pour l'ouvrir.
4. Choisissez la manière dont vous souhaitez supprimer des preuves de votre rapport d'évaluation.

   a. Pour supprimer un dossier de preuves complet, faites défiler l'écran vers le bas jusqu'à Dossiers de preuves, sélectionnez le dossier que vous souhaitez supprimer, puis choisissez Supprimer du rapport d'évaluation.

      - Si le dossier que vous recherchez ne s'affiche pas, définissez le filtre déroulant sur Toutes les dates. Dans le cas contraire, les dossiers des sept derniers jours s'afficheront par défaut.
      - Si Ajouter au rapport d'évaluation est grisé, le dossier de preuves a déjà été supprimé du rapport d'évaluation.

   b. Pour supprimer des preuves spécifiques, choisissez un dossier de preuves pour ouvrir son contenu. Sélectionnez un ou plusieurs éléments dans la liste, puis choisissez Supprimer du rapport d'évaluation.

      - Si Supprimer du rapport d'évaluation est grisé, assurez-vous d'avoir coché la case à côté des preuves, puis réessayez.
5. Une fois que vous avez ajouté les preuves au rapport d'évaluation, un bandeau vert de réussite apparaît. Choisissez Afficher les preuves dans le rapport d'évaluation pour voir les preuves qui seront incluses dans votre rapport d'évaluation.
   - Vous pouvez également consulter les preuves qui seront incluses dans votre rapport d'évaluation en revenant à votre évaluation et en choisissant l'onglet de sélection du rapport d'évaluation.

Génération de rapports d'évaluation

Après avoir ajouté des preuves à votre rapport d'évaluation, vous pouvez générer le rapport d'évaluation final à partager avec vos auditeurs. Lorsque vous générez un rapport d'évaluation, il est placé dans le compartiment S3 que vous avez choisi comme destination du rapport d'évaluation.

> **Tip**
>
> Pour vous assurer que votre rapport d'évaluation est correctement généré, consultez notre Conseils de configuration pour la destination de votre rapport d'évaluation.

Pour générer un rapport d'évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation de gauche, sélectionnez Évaluations.
3. Choisissez le nom de l'évaluation pour laquelle générer un rapport d'évaluation.
4. Choisissez l'onglet de Sélection du rapport d'évaluation, puis sélectionnez Générer le rapport d'évaluation.
   - Si l'option Générer un rapport d'évaluation est grisée, cela signifie qu'aucune preuve n'a encore été ajoutée au rapport d'évaluation.
5. Dans la fenêtre contextuelle, saisissez le nom et la description du rapport d'évaluation, puis passez en revue les détails du rapport d'évaluation.
6. Choisissez Générer un rapport d'évaluation et attendez quelques minutes pendant que votre rapport d'évaluation est généré.
7. Recherchez et chargez votre rapport d'évaluation depuis la page du Centre de téléchargement de la console Audit Manager.
   - Vous pouvez également accéder au compartiment S3 de destination de votre rapport d'évaluation et charger le rapport d'évaluation à partir de là.

Le rapport d'évaluation contient une somme de contrôle pour garantir l'intégrité du rapport d'évaluation. Pour valider l'intégrité d'un rapport d'évaluation, utilisez l'API ValidateAssessmentReportIntegrity fournie par Audit Manager.

Que puis-je faire ensuite ?

Une fois que vous aurez généré un rapport d'évaluation, vous pourrez approfondir vos connaissances en vue de :

- Trouver et charger votre rapport d'évaluation : découvrir comment charger votre rapport d'évaluation depuis le centre de téléchargement ou depuis Amazon S3.
- Explorer votre rapport d'évaluation : découvrir comment naviguer dans un rapport d'évaluation et explorer son contenu.
- Valider votre rapport d'évaluation : découvrir comment utiliser l'opération d'API ValidateAssessmentReportIntegrity pour valider votre rapport d'évaluation.
- Supprimer un rapport d'évaluation indésirable : découvrir comment supprimer un rapport indésirable du centre de téléchargement ou d'Amazon S3.

Modification du statut d'une évaluation en statut inactif

Lorsque vous n'avez plus besoin de collecter des preuves pour une évaluation, vous pouvez modifier son statut en le configurant sur Inactif. Lorsque le statut d'une évaluation est configuré sur inactif, celle-ci cesse de collecter des preuves. Par conséquent, vous ne payez plus de frais pour cette évaluation.

Outre l'arrêt de la collecte de preuves, Audit Manager apporte les modifications suivantes aux contrôles inclus dans l'évaluation inactive :

- Tous les ensembles de contrôles passent au statut Vérifié.
- Tous les contrôles En cours de vérification passent au statut Vérifié.
- Les délégués chargés de l'évaluation inactive ne peuvent plus consulter ni modifier ses contrôles et ses ensembles de contrôles.

> **Warning**
>
> Cette action est irréversible. Nous vous recommandons de procéder avec prudence et de vous assurer que vous souhaitez définir votre évaluation comme étant inactif. Lorsqu'une évaluation est inactive, vous disposez d'un accès en lecture seule à son contenu. Cela signifie que vous pouvez toujours examiner les preuves précédemment collectées et générer

des rapports d'évaluation. Cependant, vous ne pouvez pas modifier l'évaluation inactive, ajouter des commentaires ou charger des preuves manuelles.

Audit Manager console

Pour modifier le statut d'une évaluation en inactif (console)

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations.
3. Choisissez le nom de l'évaluation pour l'ouvrir.
4. En haut à droite de la page, choisissez Mettre à jour le statut de l'évaluation, puis sélectionnez Inactif.
5. Choisissez Mettre à jour le statut dans la fenêtre contextuelle pour confirmer que vous souhaitez changer le statut en inactif.

Les modifications apportées à l'évaluation et à ses contrôles prennent effet au bout d'une minute environ.

AWS CLI

Pour modifier le statut d'une évaluation en inactif (AWS CLI)

1. Tout d'abord, identifiez l'évaluation que vous voulez mettre à jour. Pour ce faire, exécutez la commande list-assessments.

```
aws auditmanager list-assessments
```

La réponse renvoie une liste d'évaluations. Recherchez l'évaluation que vous souhaitez désactiver et prenez note de l'identifiant de l'évaluation.

2. Exécutez ensuite la commande update-assessment-status et spécifiez les paramètres suivants :

- `--assessment-id`— Utilisez ce paramètre pour spécifier l'évaluation que vous souhaitez désactiver.
- `--status` – Définissez cette valeur sur `INACTIVE`.

Dans l'exemple suivant, remplacez le *texte de l'espace réservé* par vos propres informations.

```
aws auditmanager update-assessment-status --assessment-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --status INACTIVE
```

Les modifications apportées à l'évaluation et à ses contrôles prennent effet au bout d'une minute environ.

Audit Manager API

Pour modifier le statut d'une évaluation en inactif (API)

1. Recherchez avec ListAssessments l'évaluation que vous souhaitez désactiver et prenez note de l'identifiant de l'évaluation.
2. Utilisez l'opération Mettre à jour le statut de l'évaluation et spécifiez les paramètres suivants :
   - assessmentId : utilisez ce paramètre pour spécifier l'évaluation que vous souhaitez désactiver.
   - statut — Définissez cette valeur sur `INACTIVE`.

Les modifications apportées à l'évaluation et à ses contrôles prennent effet au bout d'une minute environ.

Pour plus d'informations sur ces opérations d'API, cliquez sur l'un des liens précédents dans le Guide de référence de l'API AWS Audit Manager. Il inclut des informations sur l'utilisation du fonctionnement et des paramètres dans l'un des SDK AWS spécifiques au langage.

Suppression d'une évaluation

Vous pouvez supprimer toute évaluation Audit Manager dont vous n'avez plus besoin. Vous pouvez mettre à jour ce paramètre à l'aide de la console Audit Manager, du AWS Command Line Interface de l'API Audit Manager ou du (AWS CLI).

> **Warning**
>
> Cette action entraîne la suppression définitive de votre évaluation et de toutes les preuves qu'elle a collectées. Vous ne pouvez pas récupérer ces données. Par conséquent, nous vous recommandons de procéder avec prudence et de vous assurer que vous souhaitez supprimer votre évaluation.

Audit Manager console

Pour supprimer une évaluation (console)

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations.
3. Sélectionnez l'évaluation que vous souhaitez supprimer, puis choisissez Supprimer.
   - Vous pouvez également ouvrir l'évaluation, puis choisir Supprimer en haut à droite de la page.

AWS CLI

Pour supprimer une évaluation (AWS CLI)

1. Tout d'abord, identifiez l'évaluation que vous voulez supprimer. Pour ce faire, exécutez la commande list-assessments.

   ```
   aws auditmanager list-assessments
   ```

   La réponse renvoie une liste d'évaluations. Recherchez l'évaluation que vous souhaitez supprimer et prenez note de l'identifiant de l'évaluation.
2. Ensuite, utilisez la commande delete-assessment et précisez `--assessment-id` l'évaluation que vous souhaitez supprimer.

   Dans l'exemple suivant, remplacez le *`texte de l'espace réservé`* par vos propres informations.

```
aws auditmanager delete-assessment --assessment-id a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111
```

Audit Manager API

Pour supprimer une évaluation (API)

1. Utilisez l'opération ListAssessments pour rechercher l'évaluation que vous souhaitez supprimer.

   Prenez note de l'ID d'évaluation figurant dans la réponse.
2. Utilisez l'opération DeleteAssessment et précisez l'identifiant d'évaluation que vous souhaitez supprimer.

Pour plus d'informations sur ces opérations d'API, cliquez sur l'un des liens précédents dans le Guide de référence de l'API AWS Audit Manager. Il inclut des informations sur l'utilisation du fonctionnement et des paramètres dans l'un des SDK AWS spécifiques au langage.

> **Tip**
>
> Si votre objectif est de réduire les coûts, au lieu de supprimer une évaluation, vous pouvez modifier son statut en le configurant sur inactif. Cette action met fin à la collecte de preuves et place votre évaluation dans un état de lecture seule par lequel vous pouvez consulter les preuves précédemment collectées. Les évaluations inactives n'entraînent aucuns frais.

La délégation dans AWS Audit Manager

Les responsables d'audit utilisent AWS Audit Manager pour créer des évaluations et rassembler des éléments probants pour les contrôles répertoriés dans cette évaluation. Les responsables d'audit peuvent parfois avoir des questions ou besoin d'aide pour valider les éléments probants d'une série de contrôles. Dans ce cas, le responsable de l'audit peut déléguer un ensemble de contrôles à un expert en la matière pour vérification.

De manière générale, le processus se déroule comme suit :

1. Le responsable d'audit choisit une série de contrôles dans son évaluation et la délègue pour examen.
2. Le délégué examine les contrôles et leurs éléments probants, et renvoie la série de contrôles au responsable d'audit une fois terminé.
3. Le responsable d'audit est informé que la révision est terminée et consulte les remarques éventuelles laissées par le délégué concernant les contrôles examinés.

Consultez les sections suivantes de ce guide pour en savoir plus sur la gestion des tâches de délégation dans AWS Audit Manager.

Rubriques

- Délégation des tâches des responsables d'audit
- Tâches de délégation pour les délégués

> **Note**
>
> Un même compte peut être responsable d'audit ou délégué dans différentes régions AWS.

Délégation des tâches des responsables d'audit

En tant que responsable d'audit dans AWS Audit Manager, vous pourriez avoir besoin de l'assistance d'un expert pour vous aider à examiner les contrôles et les éléments probants. Dans ce cas, vous pouvez déléguer une série de contrôles pour examen.

Les rubriques suivantes décrivent comment vous pouvez gérer les délégations dans AWS Audit Manager.

Tâches de délégation

- Délégation d'un ensemble de contrôles à des fins d'examen
- Accès à vos délégations actives et terminées
- Supprimer vos délégations actives et terminées

Délégation d'un ensemble de contrôles à des fins d'examen

Si vous avez besoin de l'aide d'un expert, vous pouvez choisir le compte AWS qui vous intéresse, puis lui déléguer une série de contrôles pour examen.

Vous pouvez utiliser l'une des procédures suivantes pour déléguer une série de contrôles.

Délégation d'une série de contrôles sur une page d'évaluation

Pour déléguer une série de contrôles sur la page d'évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Évaluations.
3. Sélectionnez le nom de l'évaluation contenant la série de contrôles que vous souhaitez déléguer.
4. Sur la page d'évaluation, choisissez l'onglet Contrôles. Le résumé de l'état des contrôles et la liste des contrôles compris dans l'évaluation s'affichent.
5. Sélectionnez une série de contrôles, puis choisissez Déléguer cette série de contrôles.
6. Sous Sélection du délégué, une liste d'utilisateurs et de rôles s'affiche. Choisissez un utilisateur ou un rôle, ou recherchez-le dans la barre de recherche.
7. Sous Détails de la délégation, vérifiez le nom de la série de contrôles et le nom de l'évaluation.
8. (Facultatif) Sous Commentaires, ajoutez un commentaire contenant des instructions pour aider le délégué à accomplir sa tâche d'examen. N'incluez aucune information sensible dans votre commentaire.
9. Choisissez Déléguer cette série de contrôle.
10. Une bannière verte confirme que la série de contrôles a été déléguée avec succès. Choisissez Afficher la délégation pour voir la demande de délégation. Vous pouvez également consulter vos

délégations à tout moment en sélectionnant Délégations dans le volet de navigation gauche de la console AWS Audit Manager.

Délégation d'une série de contrôles sur la page des délégations

Pour déléguer une série de contrôles sur la page des délégations

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, sélectionnez Délégations.
3. Sur la page des délégations, choisissez Créer une délégation.
4. Sous Choisir une évaluation et une série de contrôles, spécifiez l'évaluation et la série 'de contrôles que vous souhaitez déléguer.
5. Sous Sélection du délégué, une liste d'utilisateurs et de rôles s'affiche. Choisissez un utilisateur ou un rôle, ou recherchez-le dans la barre de recherche.
6. (Facultatif) Sous Commentaires, ajoutez un commentaire contenant des instructions pour aider le délégué à accomplir sa tâche d'examen. N'incluez aucune information sensible dans votre commentaire.
7. Cliquez sur Créer une délégation.
8. Une bannière verte confirme que la série de contrôles a été déléguée avec succès. Choisissez Afficher la délégation pour voir la demande de délégation. Vous pouvez également consulter vos délégations à tout moment en sélectionnant Délégations dans le volet de navigation gauche de la console AWS Audit Manager.

Lorsque vous déléguez une série de contrôles pour examen, le délégué reçoit une notification et peut alors commencer à examiner la série de contrôles. Ce processus effectué par les délégués est décrit dans Tâches de délégation pour les délégués.

> **Tip**
>
> Les délégués peuvent s'abonner à une rubrique SNS pour recevoir des alertes par e-mail lorsqu'une tâche d'examen leur est déléguée. Pour plus d'informations sur la façon d'identifier et de s'abonner à la rubrique SNS associée à AWS Audit Manager, voir la section Notifications dans AWS Audit Manager.

Accès à vos délégations actives et terminées

Vous pouvez accéder à la liste de vos délégations à tout moment en sélectionnant Délégations dans le volet de navigation gauche de AWS Audit Manager. La page des délégations contient une liste de vos délégations actives et terminées, les détails suivants étant indiquées pour chaque délégation :

- Délégué à : compte AWS auquel vous avez délégué la série de contrôles.
- Date : date à laquelle vous avez délégué la série de contrôles.
- État : l'état actuel de la délégation.
- Évaluation : nom de l'évaluation avec un lien vers la page détaillée de l'évaluation.
- Série de contrôles : nom de la série de contrôles qui vous a été déléguée pour examen.

Lorsqu'une délégation est terminée, vous recevez une notification dans AWS Audit Manager. Vous pouvez également recevoir des commentaires accompagnés de remarques de la part du délégué. La procédure suivante explique comment vérifier vos notifications dans Audit Manager une fois qu'une délégation est terminée, et comment consulter les éventuels commentaires du délégué.

Pour consulter une délégation terminée et vérifier les commentaires

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation, choisissez Notifications. Ou, dans la barre clignotante bleue en haut de la page, choisissez Notifications pour ouvrir la page des notifications.
3. Dans le tableau de la page Notifications, consultez les informations suivantes :
    - Date : date de la notification.
    - Évaluation : nom de l'évaluation associée à l'ensemble de contrôles.
    - Série de contrôles : le nom de la série de contrôles.
    - Source : utilisateur ou rôle du délégué qui vous a renvoyé la série de contrôles terminée.
    - Description : remarques générales formulées par le délégué.
4. Recherchez l'évaluation et la série de contrôles que le délégué a examinée et vous a soumise, puis sélectionnez le nom de l'évaluation pour l'ouvrir.
5. Sous l'onglet Contrôles de la page détaillée de l'évaluation, faites défiler la page vers le bas jusqu'au tableau Séries de contrôles. Dans la colonne Contrôles regroupés par séries

de contrôles, cliquez sur le nom d'une série de contrôles pour en afficher le détail. Puis, sélectionnez le nom d'un contrôle pour ouvrir sa page détaillée.

6. Cliquez sur l'onglet Commentaires pour afficher les remarques ajoutées par le délégué pour ce contrôle en particulier.
7. Lorsque vous êtes certain que la révision d'une série de contrôles est terminée, sélectionnez-la, puis cliquez sur Terminer l'examen de la série de contrôles.

> **Important**
>
> Audit Manager recueille des éléments probants en permanence. Par conséquent, de nouveaux éléments probants peuvent être recueillis après que le délégué ait terminé l'examen d'un contrôle.
> Si vous souhaitez uniquement utiliser les éléments probants examinés dans vos rapports d'évaluation, vous pouvez vous référer à l'horodatage de la série de contrôles pour savoir à quel moment les éléments probants ont été examinés. Cet horodatage apparaît dans l'onglet Changelog de la page détaillée du contrôle. Il vous permettra ensuite d'identifier les éléments probants à ajouter à vos rapports d'évaluation.

Supprimer vos délégations actives et terminées

Il peut arriver que vous créiez une délégation, mais que vous n'ayez plus besoin d'aide par la suite pour examiner cette série de contrôles. Dans ce cas, vous pouvez supprimer la délégation active dans AWS Audit Manager. Vous pouvez également supprimer les délégations terminées que vous ne souhaitez plus voir apparaître sur la page des délégations.

Pour supprimer une délégation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, sélectionnez Délégations.
3. Sur la page Délégations, sélectionnez la délégation que vous souhaitez annuler, puis choisissez Supprimer la délégation.
4. Dans la fenêtre contextuelle qui apparaît, choisissez Supprimer pour confirmer votre choix.

Tâches de délégation pour les délégués

Les délégués possèdent généralement une expertise commerciale ou technique spécialisée dans plusieurs domaines. Cette expertise peut porter sur les politiques de conservation des données, les plans de formation, l'infrastructure réseau ou la gestion des identités. Les délégués peuvent aider les responsables de l'audit à examiner les éléments probants collectés pour les contrôles relevant de leur domaine d'expertise.

En tant que délégué, vous pouvez recevoir des demandes de la part de responsables d'audit, afin d'examiner les éléments probants associés à une série de contrôles. Cette demande indique que le responsable d'audit a besoin de votre aide pour valider ces éléments probants. Vous pouvez aider les responsables d'audit en examinant les séries de contrôles et les éléments probants associés, en ajoutant des commentaires, en téléchargeant des éléments probants supplémentaires et en mettant à jour le statut de chaque contrôle que vous examinez.

Les rubriques suivantes décrivent comment vous pouvez gérer les délégations dans AWS Audit Manager.

> **Note**
>
> Les responsables d'audit délèguent des séries de contrôles spécifiques, et non des évaluations complètes, pour examen. Par conséquent, les délégués ont un accès limité aux évaluations. Les délégués peuvent examiner les éléments probants, ajouter des commentaires, télécharger des éléments probants manuels et mettre à jour l'état des contrôles pour chacun des contrôles de la série. Pour plus d'informations sur les rôles et les autorisations dans Audit Manager, consultez Politiques recommandées pour les personas utilisateurs dans AWS Audit Manager.

Tâches de délégation

- Affichage de vos notifications pour les demandes de délégation entrantes
- Examen de la série de contrôles déléguée et des éléments probants connexes
- Ajout de commentaires à un contrôle
- Marquer un contrôle comme vérifié
- Renvoyez la série de contrôles vérifiée au responsable d'audit

Affichage de vos notifications pour les demandes de délégation entrantes

Lorsqu'un responsable d'audit vous demande de l'aide pour examiner une série de contrôles, vous recevez une notification vous informant qu'une série de contrôles vous a été déléguée.

> **Tip**
>
> Vous pouvez également vous abonner à une rubrique SNS pour recevoir des alertes par e-mail lorsqu'une série de contrôles vous est déléguée pour examen. Pour de plus amples informations, veuillez consulter Notifications dans AWS Audit Manager.

Pour afficher vos notifications

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Notifications. Ou, dans la barre clignotante bleue en haut de la page, choisissez Afficher la notification pour ouvrir la page des notifications.
3. Sur la page Notifications, vous pouvez consulter la liste des séries de contrôles qui vous ont été déléguées pour examen. Le tableau comprend les informations suivantes :
   - Date : date à laquelle l'ensemble de contrôles a été délégué.
   - Évaluation : nom de l'évaluation associée à l'ensemble de contrôles.
   - Série de contrôles : le nom de la série de contrôles.
   - Source : utilisateur ou rôle qui vous a délégué l'ensemble de contrôle.
   - Description : les instructions fournies par le responsable de l'audit.

Examen de la série de contrôles déléguée et des éléments probants connexes

Vous pouvez aider les responsables d'audit en vérifiant les séries de contrôles qu'ils vous ont délégués. En examinant les contrôles et leurs éléments probants, vous pouvez déterminer si une action supplémentaire est nécessaire. Ces actions supplémentaires peuvent être le téléchargement manuel d'éléments probants supplémentaires pour démontrer la conformité, ou l'ajout d'un commentaire détaillant les étapes de correction effectuées.

Pour vérifier un ensemble de contrôles

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation, choisissez Notifications. Ou, dans la barre clignotante bleue, choisissez Afficher les notifications pour ouvrir la page des notifications.
3. Sur la page Notifications, la liste des séries de contrôles qui vous ont été déléguées s'affiche. Identifiez la série de contrôles que vous souhaitez examiner et choisissez le nom de l'évaluation associée pour ouvrir sa page détaillée.
4. Sous l'onglet Contrôles de la page détaillée de l'évaluation, faites défiler la page vers le bas jusqu'au tableau Séries de contrôles.
5. Dans la colonne Contrôles regroupés par séries de contrôles, cliquez sur le nom d'une série de contrôles pour en afficher le détail, puis sur le nom d'un contrôle pour ouvrir sa page détaillée.
6. (Facultatif) Choisissez Mettre à jour le statut du contrôle pour modifier le statut du contrôle. Pendant que votre vérification est en cours, vous pouvez marquer le statut comme En cours de vérification.
7. Consultez les informations relatives au contrôle dans les onglets Dossiers d'éléments probants, Sources de données, Commentaires et Journal des modifications. Pour plus d'informations sur chacun de ces onglets et sur la façon d'interpréter cette information, consultez la section Vérification des contrôles dans une évaluation.

Pour vérifier les éléments probants d'un contrôle

1. Sur la page détaillée du contrôle, choisissez l'onglet Dossiers d'éléments probants.
2. Accédez au tableau Dossiers d'éléments probants, où la liste des dossiers contenant les éléments probants de ce contrôle est affichée. Ces dossiers sont organisés et nommés en fonction de la date à laquelle les éléments probants ont été recueillis.
3. Sélectionnez le nom d'un dossier d'éléments probants pour l'ouvrir. Puis, vous pouvez consulter un résumé de tous les éléments probants recueillis à cette date. Ce résumé comprend également le nombre total de problèmes de contrôle de conformité signalés directement par AWS Security Hub, AWS Config ou par les deux. Pour obtenir des instructions sur la façon d'interpréter les données de cette page, consultez Vérification des dossiers d'éléments probants.
4. À partir de la page récapitulative du dossier de preuves, accédez au tableau éléments probants. Dans la colonne Heure, choisissez un élément de ligne à ouvrir. Passez ensuite en revue les

détails de l'élément probant recueilli à cette heure-là. Pour obtenir des instructions sur la façon d'interpréter les données de cette page, consulter Vérification d'une preuve individuelle.

> **Tip**
>
> Bien que AWS Audit Manager collecte automatiquement des éléments probants pour de nombreux contrôles, dans certains cas, vous devrez peut-être fournir des éléments probants supplémentaires pour démontrer la conformité. Dans ces cas, vous pouvez télécharger manuellement les éléments probants. Pour obtenir des instructions, veuillez consulter la section Charger des éléments probants manuelles.

Ajout de commentaires à un contrôle

Vous pouvez ajouter des commentaires pour tous les contrôles que vous vérifiez. Ces commentaires sont visibles par le responsable de l'audit.

Pour ajouter un commentaire à un contrôle

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Notifications. Vous pouvez également choisir Afficher les notifications dans la barre clignotante bleue en haut de l'écran pour ouvrir la page des notifications.
3. Sur la page Notifications, vérifiez la liste des séries de contrôles qui vous ont été déléguées. Recherchez la série de contrôles contenant le contrôle pour lequel vous souhaitez laisser un commentaire, puis cliquez sur le nom de l'évaluation associée.
4. Choisissez l'onglet Contrôles, faites défiler l'écran vers le bas jusqu'à Ensembles de contrôles, puis sélectionnez le nom d'un contrôle pour l'ouvrir.
5. Sélectionnez l'onglet Commentaires.
6. Sous Envoyer des commentaires, saisissez votre commentaire dans la zone de texte.
7. Choisissez Soumettre un commentaire pour ajouter votre commentaire. Votre commentaire apparaît désormais dans la section Commentaires précédents de la page, avec tout autre commentaire concernant ce contrôle.

Marquer un contrôle comme vérifié

Vous pouvez indiquer la progression de votre révision en mettant à jour le statut des contrôles individuels d'une série de contrôles. La modification du statut d'un contrôle est facultative. Cependant, nous vous recommandons de modifier le statut de chaque contrôle sur Vérifié au fur et à mesure de votre vérification de ce contrôle. Quel que soit le statut de chaque contrôle individuel, vous pouvez toujours renvoyer les contrôles au responsable d'audit.

Pour marquer un contrôle comme vérifié

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Notifications. Vous pouvez également choisir Afficher les notifications dans la barre clignotante bleue en haut de l'écran pour ouvrir la page des notifications.
3. Sur la page Notifications, vérifiez la liste des séries de contrôles qui vous ont été déléguées. Recherchez la série de contrôles que vous souhaitez marquer comme vérifiée et cliquez sur le nom de l'évaluation associée.
4. Sous l'onglet Contrôles de la page détaillée de l'évaluation, faites défiler la page vers le bas jusqu'au tableau Séries de contrôles.
5. Dans la colonne Contrôles regroupés par séries de contrôles, cliquez sur le nom d'une série de contrôles pour en afficher le détail. Choisissez le nom d'un contrôle pour ouvrir la page détaillée du contrôle.
6. Choisissez Mettre à jour le statut du contrôle et remplacez le statut par Vérifié.
7. Dans la fenêtre contextuelle qui apparaît, choisissez Mettre à jour le statut du contrôle pour confirmer que vous avez terminé de vérifier le contrôle.

Renvoyez la série de contrôles vérifiée au responsable d'audit

Lorsque vous avez terminé de passer en revue les contrôles qui vous ont été délégués, envoyez la série de contrôles au responsable d'audit. Ceci met fin au processus de délégation.

Pour renvoyer une série de contrôles vérifiée au responsable de l'audit

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.

2. Dans le volet de navigation de gauche, choisissez Notifications.
3. Consultez la liste des séries de contrôles qui vous ont été déléguées. Recherchez la série de contrôles que vous souhaitez renvoyer au responsable de l’audit, puis cliquez sur le nom de l’évaluation associée.
4. Faites défiler la page jusqu’au tableau Séries de contrôles, sélectionnez la série de contrôles que vous souhaitez envoyer au responsable d’audit, puis cliquez sur Envoyer pour examen.
5. Dans la fenêtre contextuelle qui apparaît, vous pouvez ajouter des commentaires avant de choisir Envoyer pour examen. Une fois le contrôle envoyé au responsable d’audit, celui-ci peut consulter les commentaires que vous lui avez laissés.

Rapports d'évaluation

Un rapport d'évaluation résume les preuves sélectionnées qui ont été recueillies pour une évaluation. Il contient également des liens vers des fichiers PDF contenant des détails sur chaque élément de preuve. Le contenu, l'organisation et la convention de dénomination spécifiques d'un rapport d'évaluation dépendent des paramètres que vous choisissez lorsque vous générez le rapport.

Les rapports d'évaluation vous aident à sélectionner et à compiler les preuves pertinentes pour votre audit. Cependant, ils n'évaluent pas la conformité des preuves elles-mêmes. Au lieu de cela, Audit Manager fournit simplement les détails des preuves sélectionnées sous forme de sortie que vous pouvez partager avec votre auditeur.

Structure du dossier du rapport d'évaluation

Lorsque vous téléchargez un rapport d'évaluation, Audit Manager crée un dossier zip. Il contient votre rapport d'évaluation et les fichiers de preuves connexes dans des sous-dossiers imbriqués.

Le dossier zip est structuré comme suit :

- Dossier d'évaluation (exemple : `myAssessmentName-a1b2c3d4`) - Le dossier racine.
  - Dossier du rapport d'évaluation (exemple : `reportName-a1b2c3d4e5f6g7`) - Sous-dossier dans lequel se trouvent les fichiers AssessmentReportSummary.pdf, digest.txt et README.txt.
    - Dossier de preuves par contrôle (exemple : `controlName-a1b2c3d4e5f6g`) - Sous-dossier qui regroupe les fichiers de preuves en fonction du contrôle correspondant.
      - Dossier de preuves par source de données (exemple : `CloudTrail`,`Security Hub`) - Sous-dossier qui regroupe les fichiers de preuves par type de source de données.
        - Dossier de preuves par date (exemple : `2022-07-01`) - Sous-dossier qui regroupe les fichiers de preuves en fonction de la date de collecte des preuves.
          - Fichiers de preuves - Fichiers qui contiennent des détails sur des éléments de preuve individuels.

Comment naviguer dans un rapport d'évaluation

Commencez par ouvrir le dossier zip et naviguez d'un niveau vers le bas jusqu'au dossier du rapport d'évaluation. Vous trouverez ici le rapport d'évaluation au format PDF et le fichier README.txt.

Vous pouvez consulter le fichier README.txt pour comprendre la structure et le contenu du dossier zip. Il fournit également des informations de référence sur les conventions de dénomination de chaque fichier. Ces informations peuvent vous aider à accéder directement à un sous-dossier ou à un fichier de preuves si vous recherchez un élément spécifique.

Sinon, pour parcourir les preuves et trouver les informations dont vous avez besoin, ouvrez le rapport d'évaluation au format PDF. Vous obtenez un aperçu général du rapport et un résumé de l'évaluation qui a servi de base à la création du rapport.

Ensuite, utilisez la table des matières (TOC) pour explorer le rapport. Vous pouvez choisir n'importe quel contrôle hypertexte dans la table des matières pour accéder directement à un résumé de ce contrôle.

Lorsque vous êtes prêt à vérifier les détails des preuves pour un contrôle, vous pouvez le faire en choisissant le nom des preuves en lien hypertexte. Pour les preuves automatisées, le lien hypertexte ouvre un nouveau fichier PDF contenant des détails sur ces preuves. Pour les preuves manuelles, le lien hypertexte vous dirige vers le compartiment S3 qui contient les preuves.

> **Tip**
>
> La piste de navigation en haut de chaque page indique votre position actuelle dans le rapport d'évaluation lorsque vous parcourez les contrôles et les preuves. Sélectionnez le lien hypertexte de la table des matières pour revenir à cette dernière à tout moment.

Sections de rapport d'évaluation

Utilisez les informations suivantes pour en savoir plus sur chaque section d'un rapport d'évaluation.

> **Note**
>
> Lorsqu'un trait d'union (-) apparaît à côté de l'un des attributs dans les sections suivantes, cela indique que la valeur de cet attribut est nulle ou qu'il n'existe aucune valeur.

- Page de couverture
- Page d'aperçu
- Page de table des matières

- Page de contrôle
- Page récapitulative des preuves
- Page détaillée des preuves

Page de couverture

La page de couverture inclut le nom du rapport d'évaluation. Elle affiche également la date et l'heure de génération du rapport, ainsi que l'ID de compte de l'utilisateur qui a généré le rapport.

La page de couverture est formatée comme suit. Audit Manager remplace les *espaces réservés* par les informations pertinentes pour votre rapport.

```
Assessment report name
Report generated on MM/DD/YYYY at HH:MM:SS AM/PM UCT by AccountID
```

Page d'aperçu

La page d'aperçu comporte deux parties : un résumé du rapport lui-même et un résumé de l'évaluation faisant l'objet du rapport.

Rapports récapitulatifs

Cette section résume le rapport d'évaluation.

- Nom du rapport - Nom du rapport.
- Description - Description saisie par le propriétaire de l'audit lorsqu'il génère le rapport.
- Date de génération - Date à laquelle le rapport a été généré. L'heure est représentée au format UTC (temps universel coordonné).
- Nombre total de contrôles inclus - Le nombre de contrôles inclus dans le rapport et pour lesquels des preuves ont été recueillies. Il s'agit d'un sous-ensemble du nombre total de contrôles inclus dans l'évaluation.
- Comptes AWS inclus — Nombre de Comptes AWS inclus dans le rapport et ayant recueilli des preuves. Il s'agit d'un sous-ensemble du nombre total de Comptes AWS dans l'évaluation.
- Sélection du rapport d'évaluation - Nombre d'éléments de preuve sélectionnés pour être inclus dans le rapport. Cela inclut le nombre total de problèmes de vérification de conformité détectés dans le rapport.

Résumé de l'évaluation

Cette section résume l'évaluation à laquelle se rapporte le rapport.

- Nom de l'évaluation - Nom de l'évaluation à partir de laquelle le rapport a été généré.
- État - État de l'évaluation au moment où le rapport a été généré.
- Région d'évaluation - Région AWS dans laquelle l'évaluation a été créée.
- Comptes AWS inclus - Liste complète de Comptes AWS inclus dans la portée de l'évaluation.
- Services AWSinclus - Liste complète de Services AWS inclus dans la portée de l'évaluation.
- Nom du framework - Nom du framework à partir duquel l'évaluation a été créée.
- Propriétaires de l'audit - Utilisateur ou rôle des responsables de l'audit de l'évaluation.
- Date de la dernière mise à jour - Date de la dernière mise à jour de l'évaluation. L'heure indique l'heure UTC.

Page de table des matières

La table des matières affiche le contenu complet du rapport d'évaluation. Le contenu est regroupé et organisé en fonction des ensembles de contrôle inclus dans l'évaluation. Les commandes sont répertoriées sous leur ensemble de commandes respectif.

Choisissez n'importe quel élément dans la table des matières pour accéder directement à cette section du rapport. Vous pouvez choisir un ensemble de commandes ou accéder directement à une commande.

Page de contrôle

La page de contrôle comporte deux parties : un résumé du contrôle lui-même et un résumé des preuves collectées pour le contrôle.

Résumé des contrôles

Cette section comprend les informations suivantes.

- Nom du contrôle : le nom du contrôle.
- Description — Description du contrôle.
- Ensemble de contrôles - Nom de l'ensemble de contrôles auquel appartient le contrôle.

- Informations de test : procédures de test recommandées pour ce contrôle.
- Plan d'action - Actions recommandées à effectuer si le contrôle n'est pas probant.
- Sélection du rapport d'évaluation - Nombre d'éléments de preuve liés à ce contrôle qui ont été inclus dans le rapport d'évaluation. Cela inclut le nombre de problèmes de contrôle de conformité détectés pour les preuves de ce contrôle.

Preuves recueillies

Cette section présente les preuves recueillies pour le contrôle. Les preuves sont regroupées par dossiers, qui sont organisés et nommés en fonction de la date de collecte des preuves. À côté du nom de chaque dossier de preuves figure le nombre total de problèmes de contrôle de conformité pour ce dossier.

Sous le nom de chaque dossier de preuves se trouve une liste de noms de preuves liés par des hyperliens.

- Les noms de preuves automatisés commencent par un horodatage de collecte de preuves, suivi du code de service, du nom de l'événement (jusqu'à 20 caractères), de l'identifiant du compte et d'un identifiant unique à 12 caractères.

  Par exemple : `21-30-24_IAM_CreateUser_111122223333_a1b2c3d4e5f6`

  Pour les preuves automatisées, le nom du lien hypertexte ouvre un nouveau fichier PDF contenant un résumé et des informations supplémentaires.
- Les noms de preuves manuels commencent par un horodatage de téléchargement des preuves, suivi de l'étiquette `manual`, de l'identifiant du compte et d'un identifiant unique à 12 caractères. Ils incluent également les 10 premiers caractères du nom du fichier, ainsi que l'extension du fichier (10 caractères maximum).

  Par exemple : `00-00-00_manual_111122223333_a1b2c3d4e5f6_myimage.png`

  Pour les preuves manuelles, le nom du lien hypertexte vous dirige vers le compartiment S3 qui contient les preuves.

À côté de chaque nom de preuve figure le résultat du contrôle de conformité de cet élément.

- Pour les preuves automatisées collectées auprès de AWS Security Hub ou de AWS Config, un résultat conforme, non conforme ou non concluant est signalé.

- Pour les preuves automatisées collectées à partir de AWS CloudTrail et d'appels d'API, et pour toutes les preuves manuelles, un résultat non concluant est affiché.

Page récapitulative des preuves

La page récapitulative des preuves comprend les informations suivantes :

- ID - Identifiant unique de la preuve.
- Date de collecte- Date à laquelle les preuves ont été créées ou téléchargées.
- Description - Description des preuves, y compris l'identifiant du compte et le type de source de données.
- Nom de l'évaluation - Nom de l'évaluation à partir de laquelle le rapport a été généré.
- Nom du framework - Nom du framework à partir duquel l'évaluation a été créée.
- Nom du contrôle - Nom du contrôle étayé par la preuve.
- Nom du jeu de contrôles - Nom de l'ensemble de contrôles auquel appartient le contrôle associé.
- Description du contrôle - Description du contrôle étayée par la preuve.
- Informations de test - Procédures de test recommandées pour le contrôle.
- Plan d'action - Actions recommandées à effectuer si le contrôle n'est pas probant.
- Région AWS - Nom de la région associée à la preuve.
- ID IAM - ARN de l'utilisateur ou du rôle associé aux preuves.
- Compte AWS - Identifiant Compte AWS associé à la preuve.
- Service AWS - Nom de Service AWS associé à la preuve.
- Ressources incluses — Les ressources AWS qui ont été évaluées pour générer la preuve. Cet attribut ne s'applique pas à la preuve de contrôle de conformité provenant deAWS Config. Pour ce type de preuve, vous pouvez trouver toutes les ressources sous forme de tableau dans le PDF Page détaillée des preuves des preuves.
- Nom de l'événement : nom de l'événement de preuve.
- Heure de l'événement - Heure à laquelle l'événement s'est produit.
- Source de données - L'endroit d'où les preuves ont été collectées ou téléchargées. Le type de source de données peut être AWS Config, Security Hub, appels AWS d'API, CloudTrail ou Manual.
- Preuve par type - Catégorie de preuve

  - Les preuves du contrôle de conformité sont collectées auprès de AWS Config ou Security Hub.
  - Les preuves de l'activité des utilisateurs sont collectées à partir des journaux CloudTrail.
  - Les preuves des données de configuration sont collectées à partir d'instantanés d'autres Services AWS.
  - Les preuves manuelles sont des preuves que vous chargez manuellement.
- Statut du contrôle de conformité - Statut d'évaluation des preuves relevant de la catégorie du contrôle de conformité.
  - Pour les preuves automatisées collectées auprès de AWS Security Hub ou de AWS Config, un résultat conforme, non conforme ou non concluant est signalé.
  - Pour les preuves automatisées collectées à partir de AWS CloudTrail et d'appels d'API, et pour toutes les preuves manuelles, un résultat non concluant est affiché.

Page détaillée des preuves

La page détaillée des preuves indique le nom de la preuve et un tableau détaillé des preuves. Ce tableau fournit une analyse détaillée de chaque élément de preuve afin que vous puissiez comprendre les données et valider leur exactitude. En fonction de la source de données des preuves, le contenu de la page détaillée des preuves varie.

> **Tip**
>
> La piste de navigation en haut de chaque page indique votre position actuelle dans le rapport d'évaluation lorsque vous parcourez les preuves détaillées. Sélectionnez Résumé des preuves pour revenir au résumé des preuves à tout moment.

Contrôle de l'intégrité du rapport d'évaluation

Lorsque vous générez un rapport d'évaluation, Audit Manager produit une somme de contrôle du fichier de rapport appelée `digest.txt`. Vous pouvez utiliser ce fichier pour valider l'intégrité du rapport et vous assurer qu'aucune preuve n'a été modifiée après la création du rapport. Il contient un objet JSON avec des signatures et des hachages qui sont invalidés si une partie de l'archive de rapports est modifiée.

Pour valider l'intégrité d'un rapport d'évaluation, utilisez l'API ValidateAssessmentReportIntegrity fournie par Audit Manager.

Rapports d'évaluation de résolution des problèmes

Pour trouver des réponses aux questions et problèmes courants, consultez la section Résolution des problèmes de rapport d'évaluation dans la section Résolution de ce guide.

Outil de recherche d'éléments probants

L'outil de recherche d'éléments probants est un puissant moyen de rechercher des éléments probants dans Audit Manager. Au lieu de parcourir des dossiers d'éléments probants profondément enfouis et difficiles d'accès pour trouver ce que vous recherchez, l'outil de recherche d'éléments probants est beaucoup plus rapide. Si vous utilisez la recherche d'éléments probants en tant qu'administrateur délégué, vous pouvez inclure tous les comptes membres de votre organisation dans votre recherche.

Vous pouvez affiner votre recherche à l'aide de filtres et de regroupements. Par exemple, si vous souhaitez obtenir une vue d'ensemble de l'état de votre système, effectuez une recherche approfondie et filtrez par évaluation, plage de dates et conformité des ressources. Si votre objectif est de remédier à une ressource spécifique, vous pouvez effectuer une recherche précise afin de cibler les preuves d'un contrôle ou d'un identifiant de ressource spécifique. Après avoir défini vos filtres, vous pouvez regrouper puis prévisualiser les résultats de recherche correspondants, avant de créer un rapport d'évaluation.

Pour utiliser l'outil de recherche d'éléments probants, vous devez activer cette fonctionnalité dans les paramètres de l'Audit Manager.

Rubriques

- Maîtriser l'outil de recherche d'éléments probants, avec CloudTrail Lake
- Activation de l'outil de recherche d'éléments probants
- Résolution des problèmes liés à l'outil de recherche d'éléments probants
- Recherchez des éléments probants
- Affichage des résultats dans l'outil de recherche d'éléments probants
- Options de filtres et de regroupement
- Exemples de cas d'utilisation

Maîtriser l'outil de recherche d'éléments probants, avec CloudTrail Lake

L'outil de recherche d'éléments probants utilise les capacités de requête et de stockage de AWS CloudTrail Lake. Avant de commencer à utiliser l'outil de recherche de preuves, il est utile d'en savoir un peu plus sur le fonctionnement de CloudTrail Lake.

CloudTrail Lake regroupe les données dans un magasin de données d'événements unique et consultable, prenant en charge de puissantes requêtes SQL. Vous pouvez ainsi effectuer des recherches dans toute votre organisation et sur des plages horaires personnalisées. L'outil de recherche d'éléments probants vous permet d'utiliser cette fonctionnalité de recherche directement sur la console Audit Manager.

Lors de la demande d'activation de l'outil de recherche d'éléments probants, Audit Manager crée un magasin de données d'événements en votre nom. Une fois l'outil de recherche d'éléments probants activé, tous vos futurs éléments probants Audit Manager sont ingérés dans le magasin de données d'événements, où ils sont disponibles pour recherche. Une fois l'outil de recherche d'éléments probants activé, la banque de données d'événements nouvellement créée se remplit automatiquement des éléments probants de ces deux dernières années. Si vous activez l'outil de recherche d'éléments probants en tant qu'administrateur délégué, les données de tous les comptes membres de votre organisation seront renseignées.

Toutes vos données d'éléments probants, qu'elles soient remplies rétroactivement ou nouvelles, sont conservées dans le magasin de données événementielles pendant 2 ans. Vous pouvez modifier la période de conservation par défaut à tout moment. Pour des instructions plus détaillées, consultez la section Mettre à jour une banque de données d'événements du guide de l'utilisateur AWS CloudTrail. Vous pouvez conserver les données d'événement dans un magasin de données d'événement pendant sept ans maximum (soit 2 555 jours).

> **Note**
>
> Le processus de remplissage rétroactif des données, lorsque cette fonctionnalité est activée, est gratuit s'il est effectué d'ici novembre 2023.
> Pour les nouveaux éléments probants ajoutés à la banque de données d'événements après cette date, CloudTrail Lake des facture des frais de stockage et d'ingestion des données.
> Les requêtes CloudTrail Lake sont payées à l'utilisation. Cela signifie que pour chaque recherche effectuée dans l'outil de recherche d'éléments probants, les données numérisées vous sont facturées.
> Pour plus d'informations sur la tarification CloudTrail Lake, consultez la section Tarification de AWS CloudTrail.

Activation de l'outil de recherche d'éléments probants

Vous pouvez activer l'outil de recherche d'éléments probants dans les paramètres d'Audit Manager. Pour obtenir des instructions, consultez la section Outil de recherche d'éléments probants sur la page Paramètres AWS Audit Manager de ce guide.

Résolution des problèmes liés à l'outil de recherche d'éléments probants

Pour trouver des réponses aux questions et problèmes courants, consultez la section Résolution des problèmes liés à l'outil de recherche d'éléments probants dans la section Dépannage de ce guide.

Recherchez des éléments probants

Pour rechercher des éléments probants sur la console Audit Manager, procédez comme suit.

> **Note**
>
> Vous pouvez également utiliser l'API CloudTrail pour interroger vos données d'éléments probants. Pour plus d'informations, consultez la section StartQuery du document Référence d'API AWS CloudTrail. Si vous préférez utiliser l'AWS CLI, voir Lancer une requête dans le guide de l'utilisateur AWS CloudTrail.

Sur cette page

- Exécution d'une requête de recherche
- Interrompre une requête de recherche
- Modification des filtres de recherche

Exécution d'une requête de recherche

Pour effectuer une recherche dans l'outil de recherche d'éléments probants, procédez comme suit.

Recherchez des éléments probants

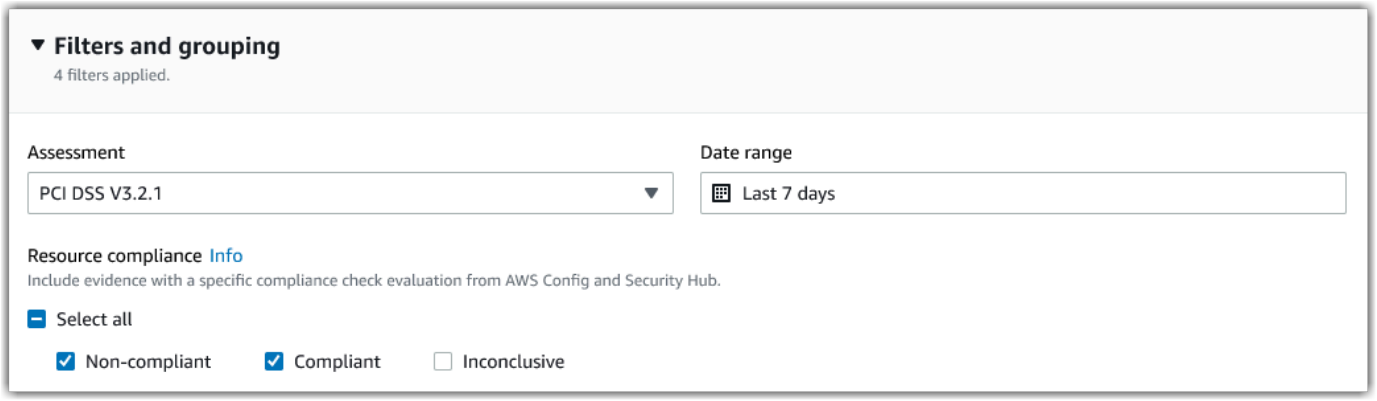
1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.

2. Dans le volet de navigation, cliquez sur Outil de recherche d'éléments probants.
3. Puis, appliquez des filtres pour réduire la portée de votre recherche.

   a. Dans Évaluation, choisissez une évaluation.

   b. Dans Plage de dates, sélectionnez une plage.

   c. Dans Conformité des ressources, sélectionnez un statut d'évaluation.

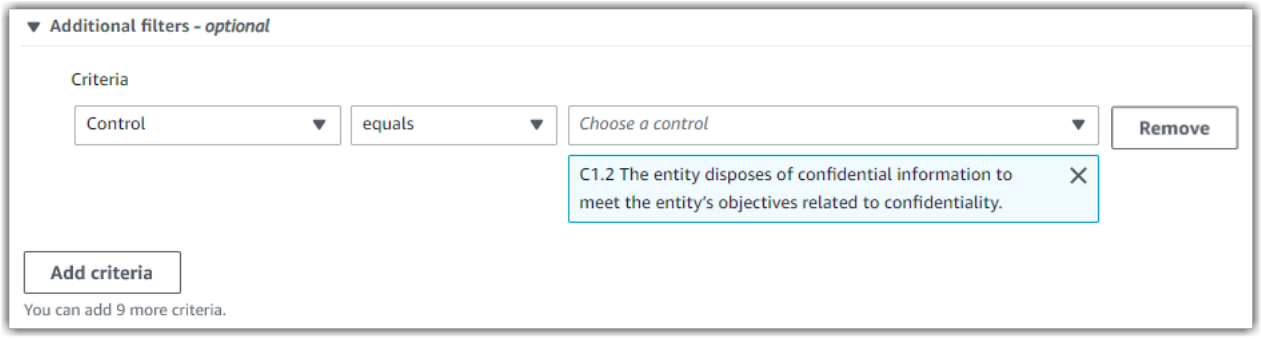


4. (Facultatif) Cliquez sur Filtres supplémentaires - facultatif pour affiner encore davantage la recherche.

   a. Cliquez surAjouter des critères, sélectionnez un critère, puis une ou plusieurs valeurs pour ce critère.

   b. Continuez à créer d'autres filtres de la même manière.

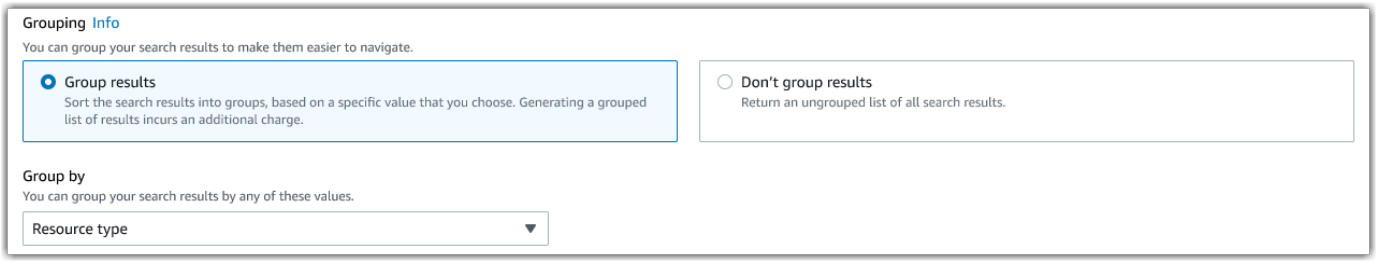
   c. Pour supprimer un filtre indésirable, cliquez sur Supprimer.



5. Sous Regroupement, indiquez si vous souhaitez regrouper les résultats de la recherche.

   a. Si vous souhaitez regrouper les résultats, sélectionnez une valeur selon laquelle les résultats seront regroupés.

b. Si vous ne souhaitez pas regrouper les résultats, passez à l'étape 6.



6. Choisissez Rechercher.

Votre recherche peut prendre quelques minutes, en fonction du nombre d'éléments probants dont vous disposez. N'hésitez pas à quitter l'outil de recherche d'éléments probants en cours de recherche. Une barre clignotante vous avertit lorsque les résultats de la recherche sont prêts.

> **Tip**
>
> Pour plus d'informations sur les filtres et les regroupements que vous pouvez utiliser dans cette procédure, consultez la section Options de filtrage et de regroupement.

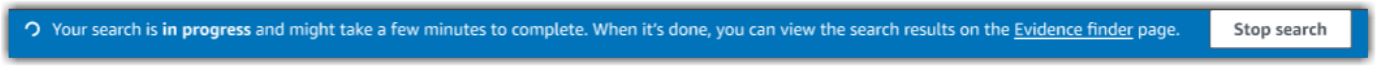
Interrompre une requête de recherche

Si vous souhaitez interrompre une requête de recherche pour une raison ou une autre, procédez comme suit.

> **Note**
>
> Même si elle est interrompue, une requête de recherche peut entraîner des frais. Le nombre d'éléments probants analysés avant l'interruption de la requête de recherche vous sera facturé. Une fois l'opération interrompue, vous pouvez consulter les résultats partiels renvoyés.

Pour interrompre une requête de recherche en cours

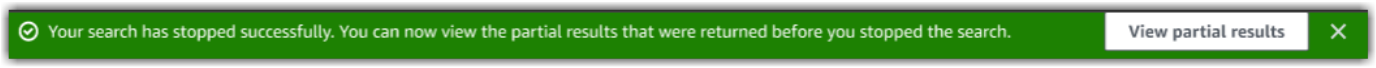
1. Dans la barre de progression bleue située en haut de l'écran, choisissez Arrêter la recherche.



2. (Facultatif) Vérifiez les résultats partiels renvoyés avant l'arrêt de la requête de recherche.

   a. Si vous êtes sur la page de l'outil de recherche d'éléments probants, les résultats partiels s'affichent à l'écran.

   b. Si vous avez quitté l'outil de recherche de preuves, choisissez Afficher les résultats partiels dans la barre de confirmation verte.



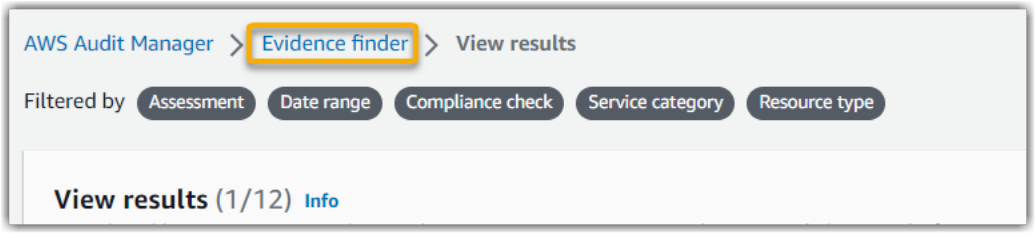
Modification des filtres de recherche

Vous pouvez revenir à votre dernière requête de recherche et modifier les filtres selon vos besoins.

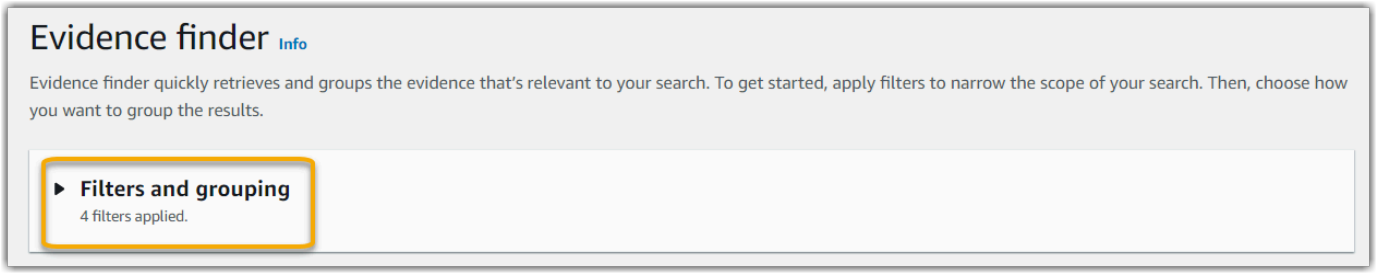
> **Note**
>
> Si vous modifiez vos filtres et que vous choisissez Rechercher, une nouvelle requête de recherche est lancée.

Pour modifier une requête de recherche récente

1. Sur la page Afficher les résultats, choisissez l'outil de recherche de preuves dans la piste de navigation.



2. Pour développer la sélection de filtres, cliquez sur Filtres et regroupements.



3. Modifiez ensuite vos filtres ou lancez une nouvelle recherche.

   a. Pour modifier les filtres, ajustez ou supprimez les filtres et la sélection de groupes actuels.

   b. Pour recommencer, cliquez sur Effacer les filtres et appliquez les filtres et les regroupements de votre choix.

4. Lorsque vous avez terminé, sélectionnez Recherche.

Affichage des résultats dans l'outil de recherche d'éléments probants

Une fois votre recherche terminée, vous pouvez consulter les résultats correspondant à vos critères de recherche.

N'oubliez pas que plusieurs ressources peuvent être évaluées lors du recueil d'éléments probants. Par conséquent, ceux-ci peuvent inclure une ou plusieurs ressources connexes. Dans l'outil de recherche d'éléments probants, les résultats s'affichent par ressource, chaque ligne correspondant à une ressource. Vous pouvez prévisualiser un résumé de chaque ressource sans quitter la page.

Après avoir examiné les résultats de la recherche, vous pouvez générer un rapport d'évaluation comprenant ces éléments probants. Vous pouvez également exporter les résultats de votre recherche dans un fichier CSV (valeurs séparées par des virgules).

> **Important**
>
> Nous vous recommandons de laisser l'outil de recherche de preuves ouvert jusqu'à ce que vous ayez fini d'explorer les résultats de la recherche. Si vous quittez le tableau Afficher les résultats, les résultats de votre recherche sont supprimés. Si nécessaire, vous pouvez consulter vos résultats récents dans la console CloudTrail à l'adresse https://console.aws.amazon.com/cloudtrail/. Les résultats de vos requêtes de recherche y sont conservés pendant sept jours. Cependant, n'oubliez pas qu'il n'est pas possible de générer un rapport d'évaluation à partir des résultats de recherche sur la console CloudTrail.

Sur cette page

- Affichage des résultats groupés
- Affichage des résultats de la recherche
  - Gérez vos préférences d'affichage
  - Prévisualiser les récapitulatifs de ressources
  - Générer un rapport d'évaluation à partir des résultats de votre recherche
  - Exporter les résultats de votre recherche

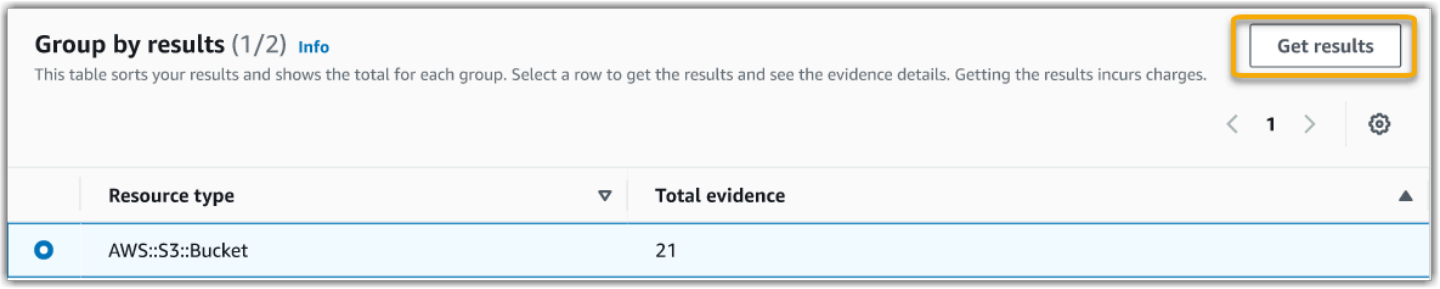
Affichage des résultats groupés

Si vous avez regroupé vos résultats, vous pouvez passer en revue ces regroupements avant d'analyser plus en profondeur les éléments probants.

> **Note**
>
> Si vous n'avez pas regroupé les résultats, l'outil de recherche d'éléments probants n'affiche pas le tableau Regrouper par résultats. Au lieu de cela, vous êtes redirigé directement vers le tableau Afficher les résultats.

Le tableau Regrouper par résultats vous indique l'étendue des éléments probants trouvés et leur répartition spécifique. Les résultats sont regroupés en fonction de la valeur sélectionnée. Par exemple, si vous avez groupé par type de ressource, le tableau affiche une liste des types de

ressources AWS. La colonne Total des preuves indique le nombre de résultats trouvés pour chaque type de ressource.



Pour obtenir les résultats d'un groupe

1. Dans le tableau Grouper par résultats, sélectionnez la ligne correspondant aux résultats que vous souhaitez obtenir.
2. Cliquez sur Obtenir les résultats. Une nouvelle requête de recherche se lance et vous êtes redirigé vers le tableau Afficher les résultats, où vous pouvez voir les résultats du groupe désiré.

Affichage des résultats de la recherche

Le tableau Afficher les résultats affiche les résultats de votre recherche. De là, vous pouvez effectuer les actions suivantes :

- Gérez vos préférences d'affichage
- Prévisualiser les récapitulatifs de ressources
- Générer un rapport d'évaluation à partir des résultats de votre recherche
- Exporter les résultats de votre recherche

Gérez vos préférences d'affichage

Vos préférences d'affichage contrôlent ce que vous voyez sur la page des résultats.

Pour gérer vos préférences d'affichage

1. Cliquez sur l'icône des paramètres (#) en haut du tableau Afficher les résultats.
2. Vérifiez et modifiez les paramètres suivants au besoin :

    a. Sélectionnez les colonnes de tableau visibles : utilisez l'option de bascule pour modifier les colonnes affichées.

b. Taille de page : sélectionnez une case d'option pour spécifier le nombre de résultats affichés sur chaque page.

c. Renvoi à la ligne : cochez cette case pour renvoyer à la ligne de longues lignes de texte, afin d'en améliorer la lisibilité.

3. Choisissez Confirmer pour enregistrer vos préférences.

Prévisualiser les récapitulatifs de ressources

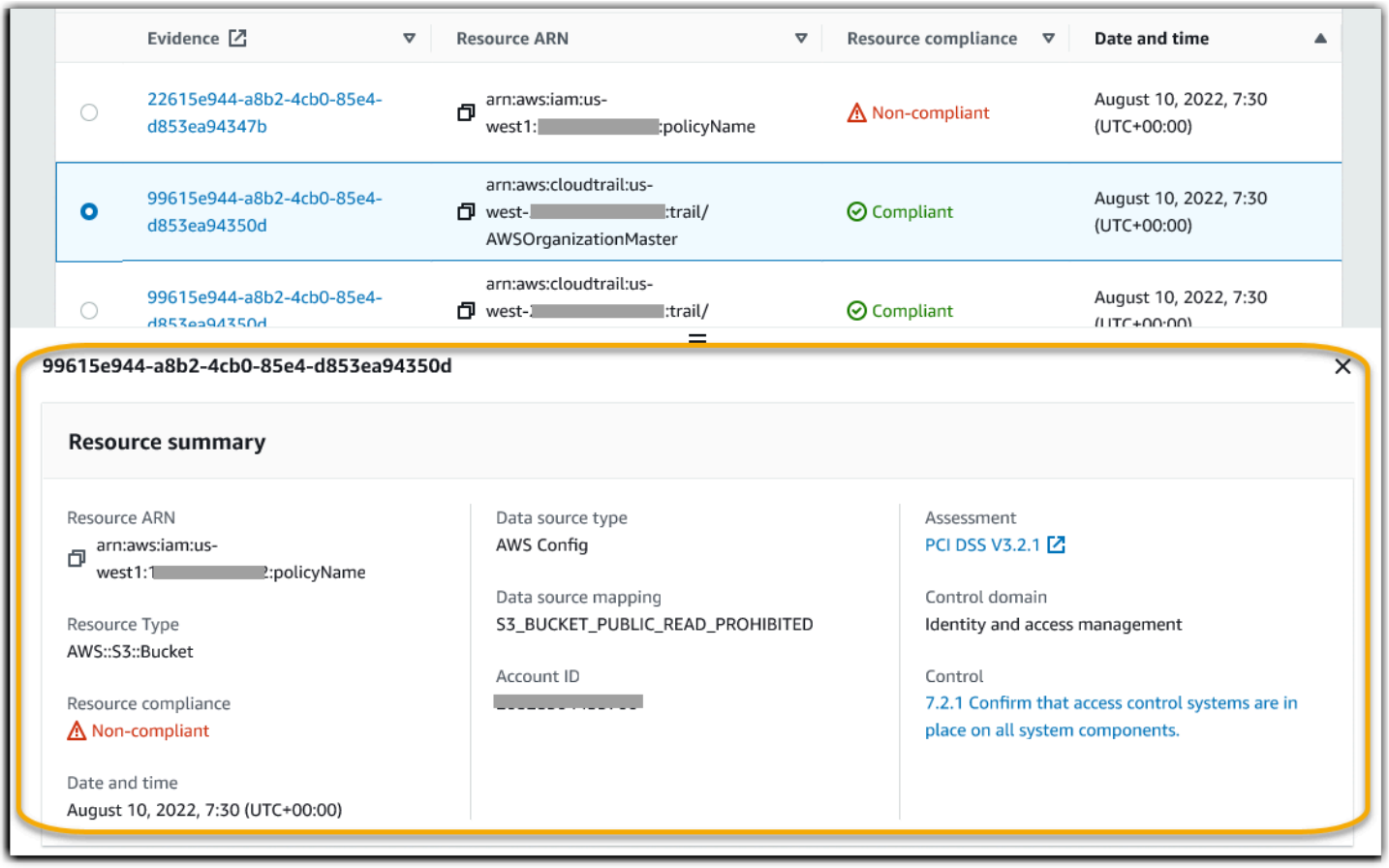
Vous pouvez prévisualiser les ressources associées aux éléments probants correspondant à votre requête de recherche. Cela vous permet de déterminer si la requête de recherche a renvoyé les résultats escomptés ou si vous devez ajuster vos filtres et réexécuter celle-ci.

N'oubliez pas que les éléments probants peuvent avoir une ou plusieurs ressources connexes. L'outil de recherche d'éléments probants affiche les résultats par ressources (une ligne par ressource).

> **Note**
>
> L'outil de recherche d'éléments probants renvoie des résultats d'éléments probants automatisés ou manuels. Toutefois, vous ne pouvez prévisualiser les récapitulatifs des ressources que pour les preuves automatisées. Cela est dû au fait qu'Audit Manager n'évalue pas les ressources pour les preuves manuelles et que, par conséquent, aucun résumé des ressources n'est disponible.
>
> Pour voir le détail d'un élément probant manuel, cliquez sur son nom : la page détaillée s'ouvre. Si vous générez un rapport d'évaluation à partir des résultats de votre recherche d'éléments probants, le détail de ceux-ci sera inclus dans le rapport d'évaluation.

Pour prévisualiser les récapitulatifs de ressources

1. Activez la case d'option située en regard d'un résultat. Un panneau récapitulatif des ressources s'ouvre sur la page en cours.
2. (Facultatif) Pour voir le détail de l'élément probant connexe, cliquez sur son nom.
3. (Facultatif) Utilisez les lignes horizontales (=) pour faire glisser et redimensionner le volet récapitulatif des ressources.
4. Cliquez sur (x) pour fermer le volet récapitulatif des ressources.



Générer un rapport d'évaluation à partir des résultats de votre recherche

Une fois que les résultats de recherche vous conviennent, générez un rapport d'évaluation.

Générer un rapport d'évaluation à partir des résultats de votre recherche

1. En haut du tableau Afficher les résultats, sélectionnez Générer un rapport d'évaluation.
2. Entrez un nom et une description pour votre rapport d'évaluation, puis passez en revue ses détails.
3. Choisissez Générer un rapport d'évaluation.

Votre rapport d'évaluation est généré en l'espace de quelques minutes. Vous pouvez, pendant ce temps ; quitter l'outil de recherche d'éléments probants : une notification verte de réussite confirmera que le rapport est prêt. Vous pouvez ensuite accéder au centre de téléchargement d'Audit Manager et télécharger votre rapport d'évaluation.

> **Note**
>
> Audit Manager génère un rapport unique à partir des éléments probants des résultats de recherche uniquement. Ce rapport ne comprend aucun élément probant ajouté manuellement à un rapport sur la page d'évaluation.
> Des limites s'appliquent au nombre d'éléments probants pouvant être inclus dans un rapport d'évaluation. Pour plus d'informations, consultez Dépannage de l'outil de recherche d'éléments probants.

Exporter les résultats de votre recherche

Vous pourrez avoir besoin d'une version portable des résultats de votre recherche. Dans ce cas, vous pouvez exporter les résultats de votre recherche dans un fichier CSV.

Une fois les résultats de votre recherche exportés, le fichier CSV sera disponible dans le centre de téléchargement d'Audit Manager pendant sept jours. Une copie de ce fichier CSV sera également envoyée vers votre compartiment S3 préféré, la destination d'exportation. Votre fichier CSV restera disponible dans ce compartiment jusqu'à ce que vous le supprimiez.

Audit Manager utilise la fonctionnalité CloudTrail Lake pour exporter et envoyer des fichiers CSV à partir de l'outil de recherche d'éléments probants. Les facteurs suivants définissent le fonctionnement du processus d'exportation au format CSV :

- Tous les résultats de votre recherche sont inclus dans le fichier CSV. Si vous souhaitez uniquement inclure des résultats de recherche spécifiques, nous vous recommandons de modifier vos filtres de recherche. Ainsi, vous pouvez affiner vos résultats pour cibler uniquement les éléments probants que vous souhaitez exporter.
- Les fichiers CSV sont exportés au format GZIP compressé. Le nom du fichier CSV par défaut est `queryID/result.csv.gz`, `queryID` étant l'ID de votre requête de recherche.
- La taille maximale d'un fichier CSV d'exportation est de 1 To. Si vous exportez plus de 1 To de données, vos résultats seront répartis dans plusieurs fichiers. Chaque fichier CSV est nommé `result_`*`number`*`.csv.gz`. Le nombre de fichiers CSV obtenu dépend de la taille totale des résultats de la recherche. Par exemple, l'exportation de 2 To de données vous fournit deux fichiers de résultats de requête : `result_1.csv.gz` et`result_2.csv.gz`.
- Outre le fichier CSV, un fichier de signature JSON est envoyé à votre compartiment S3. Ce fichier agit comme une somme de contrôle pour vérifier l'exactitude des informations contenues dans le

fichier CSV. Pour en savoir plus, consultez la structure des fichiers de signature CloudTrail dans le Guide du développeur AWS CloudTrail. La validation de l'intégrité des résultats d'une requête CloudTrail vous permet de savoir si les résultats d'une requête ont été modifiés, supprimés ou restent inchangés après envoi. Pour des instructions détaillées, consultez la section Valider les résultats des requêtes enregistrées du Guide du développeur AWS CloudTrail.

> **Note**
>
> Les réponses textuelles des preuves manuelles ne sont actuellement pas comprises dans les aperçus de l'outil de recherche de preuves, ni dans les exportations CSV. Pour voir les données de réponse textuelle, choisissez le nom de preuve manuelle dans les résultats de votre outil de recherche d'éléments probants pour ouvrir leur page détaillée. Si vous devez consulter les données des réponses textuelles en dehors de la console Audit Manager, nous vous recommandons de générer un rapport d'évaluation à partir des résultats de votre recherche d'éléments probants. Tous les détails relatifs aux éléments probants manuels, y compris les réponses textuelles, sont inclus dans les rapports d'évaluation.

Exporter vos résultats pour la première fois

Pour exporter les résultats de votre recherche pour la première fois, procédez comme suit. Cette procédure vous permet de définir une destination d'exportation par défaut pour toutes vos futures exportations. Si vous ne souhaitez pas enregistrer de destination d'exportation par défaut pour le moment, vous pouvez le faire ultérieurement en mettant à jour vos paramètres de destination d'exportation.

> **Important**
>
> Avant de commencer, assurez-vous que vous disposez d'un compartiment S3 comme destination d'exportation. Vous pouvez utiliser l'un de vos compartiments S3 existants ou créer un nouveau compartiment dans Amazon S3. En outre, votre compartiment S3 doit disposer de la politique d'autorisation requise pour permettre à CloudTrail d'y enregistrer les fichiers d'exportation. Plus précisément, la politique de compartiment doit inclure une action `s3:PutObject` et l'ARN du compartiment, et répertorier CloudTrail comme principal de service. Nous fournissons un exemple de politique d'autorisation que vous pouvez utiliser. Pour savoir comment joindre cette politique à votre compartiment S3, consultez Ajout d'une stratégie de compartiment à l'aide de la console Amazon S3.

Pour en savoir plus, consultez les conseils de configuration pour votre destination d'exportation. Si vous rencontrez des problèmes lors de l'exportation d'un fichier CSV, consultez la section Résolution des problèmes liés aux exportations CSV de l'outil de recherche d'éléments probants.

Pour exporter les résultats de votre recherche (première fois)

1. En haut du tableau Afficher les résultats, sélectionnez Exporter au format CSV.
2. Précisez le compartiment S3 vers lequel vous souhaitez exporter vos fichiers.
   - Choisissez Parcourir S3 pour sélectionner un compartiment dans la liste.
   - Vous pouvez également saisir l'URI du compartiment au format suivant : **`s3://bucketname/prefix`**

   > **Tip**
   >
   > Pour que votre compartiment de destination reste organisé, vous pouvez créer un dossier facultatif pour vos exportations CSV. Pour ce faire, ajoutez une barre oblique (**`/`**) et un préfixe à la valeur dans la zone URI de ressource (par exemple, **`/evidenceFinderExports`**). Audit Manager ajoutera alors ce préfixe lors de l'envoi du fichier CSV au compartiment et Amazon S3 génèrera le chemin spécifié par le préfixe. Pour plus d'informations sur les préfixes dans Amazon S3, veuillez consulter Organisation des objets dans la console Amazon S3 dans le Guide de l'utilisateur Amazon Simple Storage Service.
3. (Facultatif) Si vous ne souhaitez pas enregistrer ce compartiment comme destination d'exportation par défaut, décochez la case Enregistrer ce compartiment comme destination d'exportation par défaut dans les paramètres de mon outil de recherche d'éléments probants.
4. Cliquez sur Exporter.

Exporter vos résultats après avoir enregistré une destination d'exportation

Une fois votre compartiment S3 enregistré comme destination d'exportation par défaut, vous pouvez procéder comme suit.

Pour exporter les résultats de votre recherche (après avoir enregistré une destination d'exportation par défaut)

1. En haut du tableau Afficher les résultats, sélectionnez Exporter au format CSV.
2. Dans l'invite qui s'affiche, vérifiez le compartiment S3 par défaut dans lequel votre fichier exporté sera enregistré.

   a. (Facultatif) Pour continuer à utiliser ce compartiment et masquer ce message à l'avenir, cochez la case Ne plus me le rappeler.

   b. (Facultatif) Pour changer de compartiment, suivez la procédure de mise à jour de vos paramètres de destination d'exportation.
3. Choisissez Confirmer.

En fonction de la quantité de données que vous exportez, le processus d'exportation peut prendre quelques minutes. N'hésitez pas à quitter l'outil de recherche d'éléments probants pendant que l'exportation est en cours d'exécution. Si vous quittez l'outil de recherche d'éléments probants, votre recherche sera interrompue et les résultats de recherche seront ignorés dans la console. Toutefois, le processus d'exportation CSV se poursuit en arrière-plan. Le fichier CSV contiendra l'ensemble complet des résultats de recherche correspondant à votre requête.

Afficher vos résultats une fois exportés

Pour trouver votre fichier CSV et vérifier son statut, accédez au centre de téléchargement d'Audit Manager. Lorsque le fichier exporté est prêt, vous pouvez télécharger votre fichier CSV depuis le centre de téléchargement.

Vous pouvez également rechercher et télécharger le fichier CSV depuis votre compartiment S3 de destination d'exportation.

Pour rechercher votre fichier CSV et votre fichier de signature dans la console Amazon S3

1. Ouvrez la console Amazon S3.
2. Choisissez le compartiment de destination d'exportation que vous avez indiqué lors de l'exportation de votre fichier CSV.
3. Parcourez la hiérarchie des objets jusqu'à ce que vous trouviez le fichier CSV et le fichier de signature. Le fichier CSV a une extension `.csv.gz` et le fichier de signature une extension `.json`.

Vous allez parcourir une hiérarchie d'objets similaire à l'exemple suivant, mais avec un nom de compartiment de destination d'exportation, un ID de compte, une date et un ID de requête différents.

```
All Buckets
    Export_Destination_Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        YYYY
                            MM
                              DD
                                Query_ID
```

Options de filtres et de regroupement

Cette page décrit les options de filtrage et de regroupement disponibles dans l'outil de recherche d'éléments probants.

Sur cette page

- Référence du filtre
- Référence de regroupement

Référence du filtre

Vous pouvez utiliser les filtres suivants pour trouver des éléments probants correspondant à des critères spécifiques - évaluation, contrôle ou Service AWS.

Rubriques

- Filtres requis
- Filtres supplémentaires (en option)
- Filtres multiples

Filtres requis

Ces filtres vous donneront un aperçu général des éléments probants d'une évaluation pour commencer.

Nom du filtre	Description	Remarques
Évaluation	Renvoie des éléments probants pour une évaluation spécifique.	Vous pouvez filtrer en fonction d'une seule évaluation.
Plage de dates	Renvoie des éléments probants pour une période donnée.	Vous pouvez utiliser soit une plage relative, pour définir une plage de date du jour (par exemple, **`Last 30 days`**). soit une plage absolue pour spécifier une plage de dates spécifique (par exemple, **`June 27th – July 4th`**).
Conformité des ressources	Renvoie les ressources avec une évaluation de vérification de conformité spécifique.	Audit Manager recueille des preuves pour la vérification de conformité pour les contrôles utilisant AWS Config et Security Hub comme type de source de données. Plusieurs ressources peuvent être évaluées pour le recueil d'éléments probants. Par conséquent, un même élément probant pour la vérification de conformité peut comprendre une ou plusieurs ressources. Vous pouvez utiliser ce filtre pour explorer l'état de conformité par ressources. Vous pouvez choisir l'une ou plusieurs options parmi les options suivantes : • Non conforme : ce filtre trouve les ressources présentant des problèmes lors de la vérification de conformité. Cela se produit si Security Hub signale un résultat d'échec ou si AWS Config signale un résultat non conforme. • Conforme : ce filtre trouve les ressources ne présentant pas de problèmes en termes de conformité. Cela se produit si Security Hub

Nom du filtre	Description	Remarques
		signale un résultat de réussite ou si AWS Config signale un résultat conforme. • Non concluant : ce filtre trouve les ressources pour lesquelles aucune vérification de conformité n'est disponible ou applicable. Cela se produit si une ressource utilise AWS Config ou Security Hub comme type de source de données sous-jacent, mais que ces services ne sont pas activés. Cela se produit également si la ressource utilise un type de source de données sous-jacent qui ne prend pas en charge les vérifications de conformité (comme les preuves manuelles, les appels d'API AWS ou CloudTrail).

Filtres supplémentaires (en option)

Utilisez ces filtres pour affiner la portée de votre requête de recherche. Par exemple, utilisez Service pour voir toutes les preuves liées à Amazon S3. Utilisez Type de ressource pour vous limiter aux compartiments S3. Vous pouvez également utiliser Ressource ARN pour cibler un compartiment S3 spécifique.

Vous pouvez créer des filtres supplémentaires en utilisant un ou plusieurs des critères suivants.

Nom du critère	Description	Quand utiliser ce critère
ID de compte	Explorer par Compte AWS.	Utilisez ce critère pour trouver des éléments probants liés à un Compte AWS spécifique.
Contrôle	Explorer par nom de contrôle.	Utilisez ce critère pour trouver des éléments probants liés à un contrôle spécifique.

Nom du critère	Description	Quand utiliser ce critère
Domaine de contrôle	Explorer par domaine de contrôle.	Utilisez ce critère pour vous limiter à un domaine spécifiqu e pour la préparation d'un audit. Vous pouvez filtrer par domaine de contrôle si vous interrogez une évaluation créée à partir d'un framework standard. Les domaines de contrôle peuvent être, par exemple, la gestion des identités et des accès, la journalisation et la surveillance, ou la gestion du réseau.
Type de source de données	Explorer par type de source de données.	Utilisez ce critère pour vous limiter à une source de données spécifique. Définissez la valeur sur `Manual` pour rechercher les éléments probants envoyés manuellement. Sinon, vous pouvez filtrer les éléments probants automatisés en fonction de leur provenance (par exemple `AWS Config`, `CloudTrail` , `Security Hub`, ou`AWS API calls`).
Nom de l'événement	Explorer par nom d'événement.	Utilisez ce critère pour vous limiter à un événement spécifique auquel les preuves sont liées. Un événement est l'enregistrement d'une activité dans un Compte AWS. Par exemple, vous pouvez rechercher le nom d'un appel d'API, comme l'opération IAM `AttachRolePolicy` utilisée pour configurer les autorisations. Vous pouvez également rechercher un mot clé CloudTrail, comme l'événement `ConsoleLogin` consigné par CloudTrail lorsqu'un utilisateur se connecte à votre compte.
ARN des ressources	Explorer par Amazon Resource Name (ARN).	Utilisez ce critère pour trouver des éléments probants liés à une ressource AWS spécifique.

Nom du critère	Description	Quand utiliser ce critère
Type de ressource	Explorer par type de ressource.	Utilisez ce critère pour vous limiter au type de ressource évalué, comme une instance Amazon EC2 ou un compartiment S3.
Service	Explorer par nom de Service AWS.	Utilisez ce critère pour trouver des éléments probants liés à un Service AWSspécifique, comme Amazon EC2, Amazon S3 ou AWS Config.
Catégorie de services	Explorer par catégorie de Service AWS.	Utilisez ce critère pour vous concentrer sur une catégorie spécifique de Service AWS. Par exemple la sécurité, l'identité et la conformité, les bases de données et le stockage.

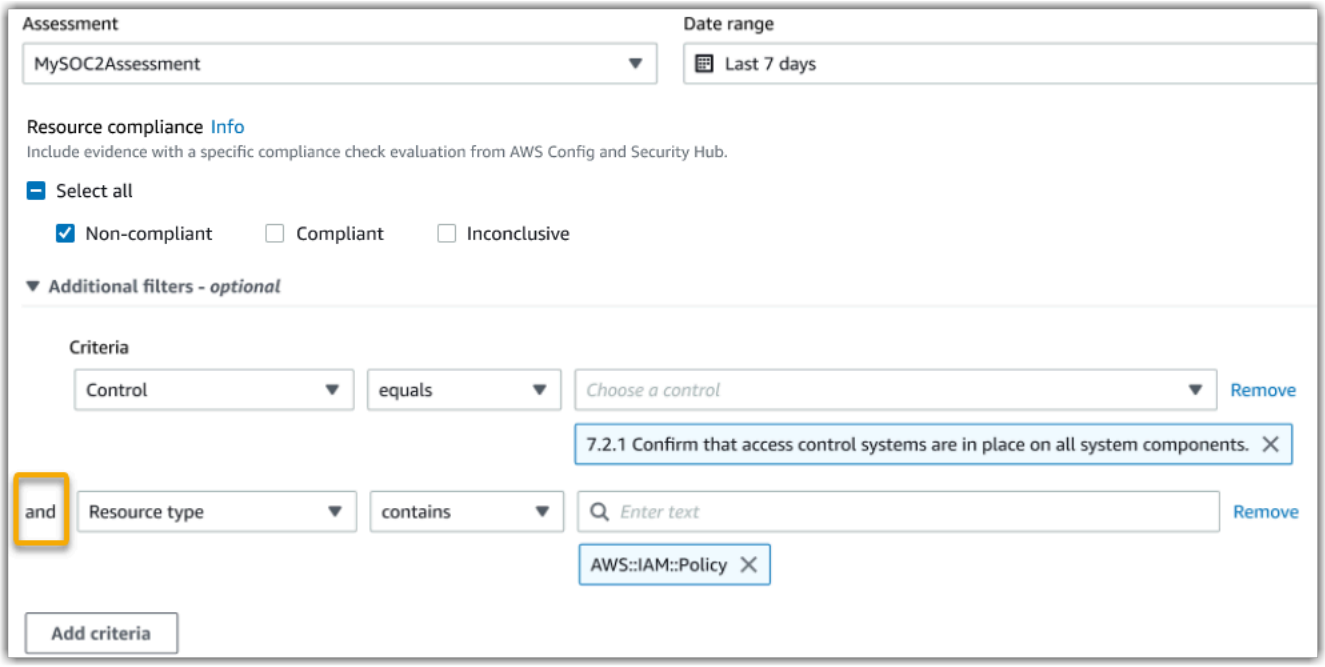
Filtres multiples

Comportement des critères

Si vous spécifiez plusieurs critères, Audit Manager applique l'opérateur `AND` à vos sélections. Cela signifie que tous les critères sont regroupés dans une seule requête et que les résultats doivent correspondre à tous les critères conjugués.

Exemple

Dans la configuration de filtre suivante, l'outil de recherche d'éléments probants renvoie les ressources non conformes des 7 derniers jours pour l'évaluation dénommée **`MySOC2Assessment`**. En outre, les résultats concernent à la fois une politique IAM et le contrôle spécifié.

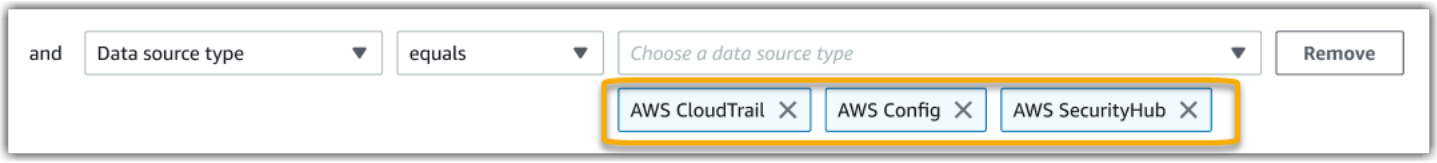


Comportement des valeurs de critère

Si vous spécifiez plusieurs valeurs de critère, ces valeurs sont liées par un opérateur `OR`. L'outil de recherche de preuves renvoie des résultats correspondant à l'une de ces valeurs de critères.

Exemple

Dans la configuration de filtre suivante, l'outil de recherche d'éléments probants renvoie des résultats de recherche provenant de AWS CloudTrail, AWS Config, ou AWS Security Hub.



Référence de regroupement

Vous pouvez regrouper les résultats de recherche pour accélérer la navigation. Le regroupement vous montre l'étendue de vos résultats de recherche et leur répartition spécifique.

Vous pouvez utiliser le regroupement par les valeurs suivantes de votre choix.

Regrouper par	Description
ID de compte	Regrouper les résultats par Compte AWS.

Regrouper par	Description
Contrôle	Regroupez les résultats par nom de contrôle.
Domaine de contrôle	Regroupez les résultats par domaine de contrôle.
Type de source de données	Regroupez les résultats par type de source de données d'où proviennent les preuves.
Nom de l'événement	Regroupez les résultats par nom d'événement.
ARN des ressources	Regroupez les résultats par Amazon Resource Name (ARN).
Type de ressource	Regroupez les résultats par type de ressource.
Service	Regroupez les résultats par nom de Service AWS.
Catégorie de services	Regroupez les résultats par catégorie de Service AWS.

Exemples de cas d'utilisation

L'outil de recherche d'éléments probants peut vous aider dans plusieurs cas d'utilisation. Cette page fournit quelques exemples et suggère les filtres de recherche que vous pouvez utiliser dans chaque scénario.

Rubriques

- Cas d'utilisation 1 : trouver des éléments probants non conformes et organiser des délégations
- Cas d'utilisation 2 : Identification des preuves de conformité
- Cas d'utilisation 3 : aperçu rapide des ressources d'éléments probants

Cas d'utilisation 1 : trouver des éléments probants non conformes et organiser des délégations

Ce cas d'utilisation est idéal si vous êtes responsable de la conformité ou de la protection des données ou un professionnel GRC chargé de superviser la préparation des audits.

Pour la surveillance du niveau de conformité de votre organisation, vous pouvez compter sur vos équipes partenaires pour vous aider à résoudre les problèmes. L'outil de recherche d'éléments probants vous aide à organiser votre travail pour vos équipes partenaires.

En appliquant des filtres, vous pouvez vous limiter aux éléments probants d'un seul domaine à la fois. De plus, vous pouvez également rester en phase avec les responsabilités et le champ d'action de chaque équipe partenaire avec laquelle vous travaillez. En effectuant une recherche ciblée de cette manière, vous pouvez utiliser les résultats de recherche pour identifier exactement ce qui doit être corrigé dans chaque domaine. Vous pouvez ensuite déléguer ces preuves non conformes à l'équipe partenaire correspondante pour qu'elle y remédie.

Pour ce flux de travail, procédez à la recherche d'éléments probants. Utilisez les filtres suivants pour rechercher des éléments probants de non-conformité.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Non-compliant
```

Appliquez ensuite des filtres supplémentaires pour le domaine choisi. Par exemple, utilisez le filtre Catégorie de service pour rechercher les ressources non-conformes liées à IAM. Partagez ensuite ces résultats avec l'équipe responsable des ressources IAM de votre organisation. Ou si vous interrogez une évaluation créée à partir d'un framework standard, vous pouvez utiliser le filtre Domaine de contrôle pour trouver des preuves de non-conformité liées au domaine de gestion des identités et des accès.

```
Control domain | <domain that you're focusing on>
or
Service category | <Service AWS category that you're focusing on>
```

Une fois trouvées les preuves dont vous avez besoin, procédez à la génération d'un rapport d'évaluation à partir des résultats de recherche. Vous pouvez partager ce rapport avec votre équipe partenaire, qui pourra l'utiliser comme liste de contrôle des mesures correctives.

Cas d'utilisation 2 : Identification des preuves de conformité

Ce cas d'utilisation est idéal si vous travaillez dans les secteurs SecOps, IT/DevOps ou si vous occupez un autre poste responsable des actifs cloud et de leur correction.

Dans le cadre d'un audit, il peut vous être demandé de résoudre des problèmes liés aux ressources dont vous êtes responsable. Une fois de travail effectué, vous pouvez valider la conformité de vos ressources à l'aide de l'outil de recherche d'éléments probants.

Pour ce flux de travail, procédez à la recherche d'éléments probants. Utilisez les filtres suivants pour rechercher des éléments probants de conformité.

```
Assessment | <assessment name>
Date range | <date range>
Resource compliance | Compliant
```

Puis, appliquez des filtres supplémentaires pour n'afficher que les éléments probants dont vous êtes responsable. Selon l'étendue de votre responsabilité, faites en sorte que la recherche soit aussi ciblée que nécessaire. Les exemples de filtres suivants vont du plus large au plus précis. Choisissez les options qui vous conviennent et remplacez-les *<placeholder text>* par vos propres valeurs.

```
Control domain | <a subject area that you're responsible for>
Service category | <a category of Services AWS that you own>
Service | <a specific Service AWS that you own>
Resource type | <a collection of resources that you own>
Resource ARN | <a specific resource that you own>
```

Si vous êtes responsable de plusieurs instances des mêmes critères (par exemple de plusieursServices AWS), vous pouvez regrouper vos résultats en fonction de cette valeur. Cela vous fournit le total des éléments probants concordants pour chaque Service AWS. Vous pouvez ensuite obtenir les résultats pour les services dont vous êtes responsable.

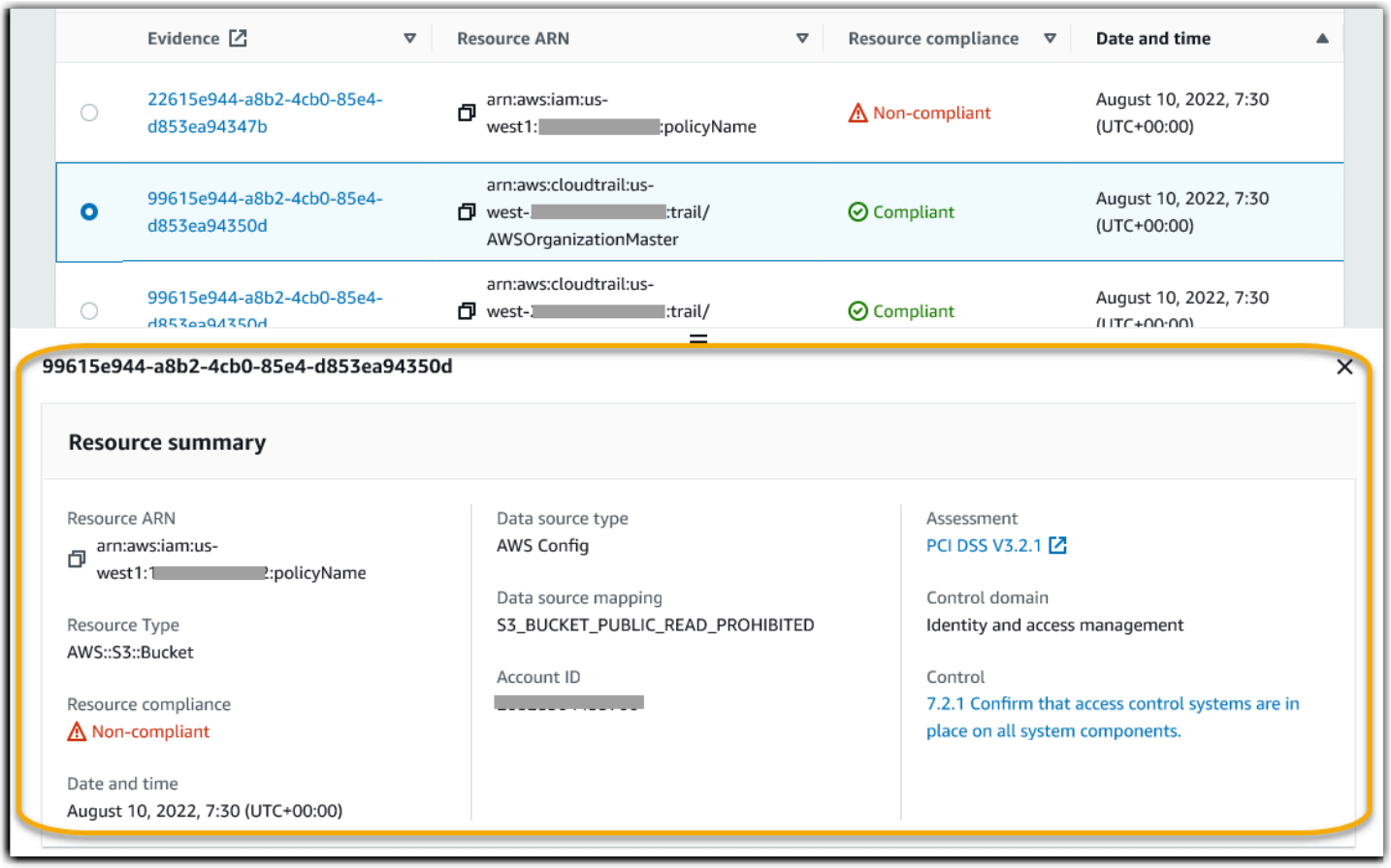
Cas d'utilisation 3 : aperçu rapide des ressources d'éléments probants

Ce cas d'utilisation est idéal pour tous les clients d'Audit Manager.

Auparavant, l'examen détaillé des éléments probants individuels prenait beaucoup de temps. Si vous vouliez avoir un aperçu des éléments probants, vous deviez accéder directement à cette évaluation, puis parcourir des dossiers d'éléments probants profondément enfouis et difficiles à trouver. Désormais, l'outil de recherche d'éléments probants est un moyen pratique de prévisualiser ces informations. Pour chaque élément probant correspondant à votre requête de recherche, vous pouvez prévisualiser les ressources individuelles correspondantes.

Pour commencer, lancez une recherche d'éléments probants. Activez ensuite la case d'option en regard d'un résultat pour afficher le récapitulatif des ressources dans la page actuelle. Vous pouvez

prévisualiser chaque ressource individuelle associée à un élément probant. Pour voir le détail complet des éléments probants de la ressource de votre choix, cliquez sur le nom de cet élément probant. Pour de plus amples informations, veuillez consulter la section Prévisualiser les récapitulatifs des ressources.



Centre de téléchargement d'Audit Manager

Le centre de téléchargement est l'endroit où vous pouvez trouver et gérer tous vos fichiers Audit Manager téléchargeables. Lorsque vous générez un rapport d'évaluation ou que vous exportez des résultats de recherche depuis Evidence Finder, les fichiers apparaissent dans le centre de téléchargement.

Rubriques

- Naviguer dans le centre de téléchargement
- Téléchargement d'un fichier
- Supprimer un fichier

Naviguer dans le centre de téléchargement

Pour accéder au centre de téléchargement, ouvrez la console Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home, puis choisissez Centre de téléchargement dans le volet de navigation de gauche.

Vous pouvez passer d'un onglet à l'autre pour parcourir vos fichiers par catégorie.

Onglet Rapports d'évaluation

Cet onglet affiche tous les rapports d'évaluation que vous avez générés. Les rapports d'évaluation restent disponibles dans le centre de téléchargement jusqu'à ce que vous les supprimiez.

Pour voir le statut le plus récent de votre rapport d'évaluation, cliquez sur l'icône d'actualisation (#) pour recharger le tableau. Chaque ligne du tableau des rapports d'évaluation indique le nom du rapport, sa date de création et l'un des statuts suivants :

- En cours — Audit Manager est en train de générer le rapport d'évaluation.
- Prêt — Vous pouvez télécharger le rapport d'évaluation.
- Erreur : le rapport d'évaluation n'a pas pu être généré. Dans ce cas, Audit Manager affiche un message décrivant l'erreur. Pour plus d'informations sur la façon de résoudre ces erreurs, consultez la section Résolution des problèmes liés aux rapports d'évaluation.

Onglet Exportations

Cet onglet affiche tous les résultats de recherche de preuves que vous avez exportés au cours des sept derniers jours. Les fichiers CSV sont supprimés du centre de téléchargement au bout de

sept jours, mais ils restent disponibles dans votre compartiment S3 de destination d'exportation. Pour obtenir des instructions sur la façon de trouver une exportation CSV de recherche de preuves dans votre compartiment de destination S3, consultez Afficher vos résultats une fois exportés.

Pour voir le statut le plus récent de vos exportations CSV, cliquez sur l'icône d'actualisation (#) pour recharger le tableau. Chaque ligne du tableau des exportations indique le nom du fichier, sa date d'exportation et l'un des statuts suivants :

- En cours — Audit Manager est en train de préparer le fichier CSV.
- Prêt — L'exportation a réussi et le fichier peut être téléchargé.
- Erreur — L'exportation a échoué. Dans ce cas, Audit Manager affiche un message décrivant l'erreur. Pour plus d'informations sur la façon de résoudre ces erreurs, consultez Résolution des problèmes d'exportation CSV de Evidence Finder.

> **Note**
>
> N'oubliez pas que l'onglet Exportations peut également afficher des fichiers CSV pour les requêtes que vous avez exécutées directement dans AWS CloudTrail Lake. Cela inclut les requêtes effectuées dans la console CloudTrail ou à l'aide de l'API CloudTrail. Les exportations CloudTrail apparaissent sous cet onglet si vous avez interrogé le magasin de données d'événements d'Audit Manager et que vous avez choisi d'enregistrer les résultats sur Amazon S3.

Téléchargement d'un fichier

Procédez comme suit pour télécharger un fichier depuis le centre de téléchargement.

Pour télécharger un fichier

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, sélectionnez Centre de téléchargement.
3. Choisissez l'onglet Rapports d'évaluation ou l'onglet Exportations.
4. Sélectionnez le fichier que vous souhaitez télécharger, puis choisissez Télécharger.

Pour savoir comment télécharger un fichier depuis votre compartiment de destination S3, consultez la section Téléchargement d'un objet dans le Guide de l'utilisateur d'Amazon Simple Storage Service (Amazon S3).

Supprimer un fichier

Suivez ces étapes pour supprimer tous les rapports d'évaluation dont vous n'avez plus besoin dans le centre de téléchargement.

> **Note**
>
> La suppression des exportations CSV du centre de téléchargement n'est actuellement pas prise en charge. Les exportations CSV sont automatiquement supprimées du centre de téléchargement au bout de sept jours.

Pour supprimer un rapport d'évaluation

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, sélectionnez Centre de téléchargement.
3. Choisissez l'onglet Rapports d'évaluation.
4. Sélectionnez le rapport d'évaluation que vous souhaitez supprimer, puis choisissez Supprimer.

Si vous souhaitez supprimer un rapport d'évaluation ou une exportation CSV depuis votre compartiment de destination S3, nous vous recommandons d'effectuer cette tâche directement dans Amazon S3. Pour obtenir des instructions, consultez la section Supprimer des objets Amazon S3 dans le Guide de l'utilisateur d'Amazon Simple Storage Service (Amazon S3).

Bibliothèque de frameworks

Vous pouvez accéder aux frameworks et les gérer à partir de la bibliothèque de frameworks dans AWS Audit Manager.

Un framework détermine les contrôles qui sont testés dans un environnement sur une période. Il définit les contrôles et leurs mappages de sources de données pour une norme ou une réglementation de conformité donnée. Il est également utilisé pour structurer et automatiser les évaluations Audit Manager. Vous pouvez utiliser des frameworks comme point de départ pour auditer votre utilisation du Service AWS et commencer à automatiser la collecte de preuves.

La bibliothèque de frameworks contient un catalogue de frameworks standard et personnalisés.

- Les frameworks standard sont des frameworks prédéfinis que AWS fournit. Ces frameworks sont basés sur les bonnes pratiques AWS relatives aux différentes normes et réglementations de conformité. Il s'agit notamment du RGPD et de HIPAA. Les frameworks standard incluent des contrôles organisés en ensembles de contrôles basés sur la norme de conformité ou la réglementation prise en charge par le framework.

  Vous pouvez consulter le contenu des frameworks standard, mais vous ne pouvez ni les modifier ni les supprimer. Cependant, vous pouvez personnaliser n'importe quel framework standard pour en créer un nouveau répondant à vos besoins spécifiques.
- Les frameworks personnalisés sont des frameworks personnalisés que vous possédez. Vous pouvez créer un framework personnalisé entièrement ou en personnalisant un framework existant. Vous pouvez utiliser des frameworks personnalisés pour organiser les contrôles en ensembles de contrôles de manière à répondre à vos exigences spécifiques. Pour en savoir sur la façon de gérer les contrôles, consultez Bibliothèque de contrôles.

Vous pouvez créer une évaluation à partir d'un framework standard ou personnalisé. Pour en savoir sur la façon de créer et de gérer des évaluations, consultez Évaluations dans AWS Audit Manager.

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

aux audits. AWS Audit Manager ne remplace pas un conseiller juridique ou un expert en conformité.

Cette section décrit comment créer et gérer des frameworks personnalisés dans Audit Manager.

Rubriques

- Accès aux frameworks disponibles dans AWS Audit Manager
- Affichage des détails d'un framework
- Création d'un framework personnalisé
- Modification d'un framework personnalisé
- Suppression d'un framework personnalisé
- Partage d'un framework personnalisé
- Frameworks pris en charge dans AWS Audit Manager

Accès aux frameworks disponibles dans AWS Audit Manager

Vous pouvez consulter tous les frameworks disponibles sur la page Bibliothèque de frameworks de la console Audit Manager. À partir de là, vous pouvez également créer une évaluation à partir d'un framework, créer un framework personnalisé ou personnaliser un framework existant.

Vous pouvez également consulter tous les frameworks disponibles à l'aide de l'API Audit Manager ou de AWS Command Line Interface (AWS CLI).

Audit Manager console

Pour afficher les frameworks disponibles (console)

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Bibliothèque de frameworks.
3. Choisissez l'onglet Frameworks standard ou Frameworks personnalisés pour parcourir les frameworks standard et personnalisés disponibles.
4. Choisissez un nom de framework pour en afficher les détails.

AWS CLI

Pour afficher les frameworks disponibles (AWS CLI)

Pour afficher les frameworks dans Audit Manager, utilisez la commande list-assessment-frameworks et spécifiez un `--framework-type`. Vous pouvez récupérer la liste des frameworks standard. Vous pouvez également récupérer la liste des frameworks personnalisés.

```
aws auditmanager list-assessment-frameworks --framework-type Standard
```

```
aws auditmanager list-assessment-frameworks --framework-type Custom
```

Audit Manager API

Pour afficher les frameworks disponibles (API)

Utilisez l'opération ListAssessmentFrameworks et spécifiez un frameworkType. Vous pouvez renvoyer la liste des frameworks standard. Vous pouvez également renvoyer la liste des frameworks personnalisés.

Pour plus d'informations, choisissez l'un des liens précédents pour en lire davantage dans le Guide de référence de l'API AWS Audit Manager. Il inclut des informations sur l'utilisation du fonctionnement et des paramètres `ListAssessmentFrameworks` dans l'un des SDK AWS spécifiques au langage.

Affichage des détails d'un framework

Vous pouvez consulter les détails d'un framework à l'aide de la console Audit Manager, de l'API Audit Manager ou de AWS Command Line Interface (AWS CLI).

Audit Manager console

Pour afficher les détails du framework (console)

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation de gauche, choisissez Bibliothèque de frameworks pour voir la liste des frameworks disponibles.

3. Choisissez l'onglet Frameworks standard ou Frameworks personnalisés pour parcourir les frameworks disponibles.
4. Choisissez le nom du framework pour l'ouvrir.

Lorsque vous ouvrez un framework, une page Détails du framework s'affiche. Les sections de cette page et leur contenu sont décrits comme suit.

Section des détails du framework

Cette section fournit une présentation du framework. Il contient les informations suivantes :

- Nom du framework : nom du framework.
- Type de conformité : norme ou réglementation de conformité prise en charge par le framework.
- Description : Description du framework, le cas échéant.
- Type de framework : Spécifie s'il s'agit d'un framework standard ou personnalisé.
- Ensembles de contrôles : nombre d'ensembles de contrôles associés au framework.
- Contrôles : nombre total de contrôles dans le framework.
- Sources de contrôle : nombre de sources de données de contrôle à partir desquelles Audit Manager collecte des preuves.
- Balises : balises associées au framework.

Si vous consultez un framework personnalisé, les informations suivantes sont également affichées :

- Créé par : compte qui a créé le framework personnalisé.
- Créé le : date à laquelle a été créé le framework personnalisé.
- Dernière mise à jour : date à laquelle ce framework a été modifié pour la dernière fois.

Onglet Contrôles

Cet onglet répertorie les contrôles du framework, regroupés par ensemble de contrôles. Il contient les informations suivantes :

- Contrôles regroupés par ensemble de contrôles : cliquez sur l'icône d'arborescence pour voir les contrôles appartenant à chaque ensemble de contrôles.
- Type : spécifie s'il s'agit d'un contrôle standard ou personnalisé.
- Source de données : spécifie la source de données à partir de laquelle Audit Manager collecte les preuves nécessaires à ce contrôle.

Onglet Balises

Cet onglet liste les balises associées au framework. Il contient les informations suivantes :

- Clé : la clé de la balise (par exemple, une norme de conformité, une réglementation ou une catégorie).
- Valeur : la valeur de la balise.

AWS CLI

Pour afficher les détails du framework (AWS CLI)

1. Pour identifier le framework que vous souhaitez examiner, exécutez la commande list-assessment-frameworks et spécifiez un `--framework-type`. Vous pouvez récupérer la liste des frameworks standard. Vous pouvez également récupérer la liste des frameworks personnalisés.

   Dans l'exemple suivant, remplacez le *texte de l'espace réservé* par `Custom` ou `Standard`.

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom/Standard
   ```

   La réponse renvoie une liste de frameworks. Recherchez le framework que vous souhaitez consulter, et prenez note de l'ID du framework et du Amazon Resource Name (ARN).
2. Pour obtenir les détails du framework, exécutez la commande get-assessment-framework et spécifiez le `--framework-id`.

   Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations.

   ```
   aws auditmanager get-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Les détails du framework sont renvoyés au format JSON. Pour comprendre ces données, consultez le résultat de get-assessment-framework dans la référence de la commande AWS CLI.
3. Pour voir les balises d'un framework, utilisez la commande list-tags-for-resource et spécifiez le `--resource-arn` du framework.

Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations :

```
aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:assessmentFramework/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Pour plus d'informations sur les balises dans l'Audit Manager, consultez Balisage des ressources AWS Audit Manager.

Audit Manager API

Pour afficher les détails du framework (API)

1. Pour identifier le framework que vous souhaitez examiner, exécutez la commande list-assessment-frameworks et spécifiez un frameworkType. Vous pouvez renvoyer la liste des frameworks standard. Vous pouvez également renvoyer la liste des frameworks personnalisés.

   Pour la réponse, recherchez le framework que vous souhaitez consulter, et prenez note de l'ID du framework et du Amazon Resource Name (ARN).

2. Pour obtenir les détails du framework, utilisez l'opération GetAssessmentFramework. Dans la demande, spécifiez le frameworkId que vous avez obtenu à l'étape 1.

   Les détails du framework sont renvoyés au format JSON. Pour comprendre ces données, consultez la section Éléments de réponse GetAssessmentFramework dans la référence de l'API AWS Audit Manager.

3. Pour voir les balises du framework, utilisez l'opération ListTagsForResource. Dans la demande, spécifiez le resourceArn du framework que vous avez obtenu à l'étape 1.

Pour plus d'informations sur les balises dans l'Audit Manager, consultez Balisage des ressources AWS Audit Manager.

Pour plus d'informations sur ces opérations d'API, cliquez sur l'un des liens précédents dans le Guide de référence de l'API AWS Audit Manager. Il inclut des informations sur l'utilisation du fonctionnement et des paramètres dans l'un des SDK AWS spécifiques au langage.

Création d'un framework personnalisé

Vous pouvez accéder aux frameworks et les gérer à partir de la bibliothèque de frameworks dans AWS Audit Manager. Vous pouvez créer des frameworks personnalisés pour organiser les contrôles en ensembles de contrôles de manière à répondre à vos exigences spécifiques.

Il existe deux façons de créer un framework personnalisé. Vous pouvez personnaliser un framework existant ou en créer un nouveau entièrement.

Rubriques

- Création d'un framework personnalisé totalement nouveau
- Personnalisation d'un framework existant

Création d'un framework personnalisé totalement nouveau

Vous pouvez utiliser des frameworks personnalisés dans AWS Audit Manager pour organiser les contrôles en ensembles de contrôles de manière à répondre à vos besoins spécifiques. Vous pouvez créer un tout nouveau framework personnalisé dans la bibliothèque de frameworks en suivant ces étapes.

Rubriques

- Étape 1 : Spécifier les détails du framework
- Étape 2 : Indiquer les contrôles dans les ensembles de contrôles
- Étape 3 : Examen et création du framework
- Que puis-je faire ensuite ?

Étape 1 : Spécifier les détails du framework

Commencez par définir les contrôles que vous souhaitez inclure dans votre framework personnalisé.

Pour spécifier les détails du framework

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Bibliothèque de frameworks, puis Créer un framework personnalisé.

3. Dans Détails du framework, entrez un nom, une norme ou une réglementation de conformité (facultatif) et une description de votre framework (également facultatif). Entrez un mot clé de norme ou de réglementation de conformité tel que PCI_DSS ou GDPR afin de pouvoir utiliser ce mot clé pour rechercher votre framework.
4. Sous Balises, choisissez Ajouter une nouvelle balise pour associer une balise à votre framework. Vous pouvez indiquer une clé et une valeur pour chaque balise. La clé de balise est obligatoire. Vous pouvez l'utiliser comme critère de recherche lorsque vous recherchez ce framework dans la bibliothèque de framework. Pour plus d'informations sur les balises dans AWS Audit Manager, consultez Balisage de ressources AWS Audit Manager.
5. Choisissez Next (Suivant).

Étape 2 : Indiquer les contrôles dans les ensembles de contrôles

Ensuite, vous spécifiez les contrôles que vous souhaitez ajouter à votre framework et la manière dont vous souhaitez les organiser. Commencez par ajouter des ensembles de contrôles au framework, puis ajoutez des contrôles à l'ensemble de contrôles.

> **Note**
>
> Lorsque vous utilisez la console AWS Audit Manager pour créer un framework personnalisé, vous pouvez ajouter jusqu'à 10 ensembles de contrôles pour chaque framework.
> Lorsque vous utilisez l'API Audit Manager pour créer un framework personnalisé, vous pouvez créer plus de 10 ensembles de contrôles. Pour ajouter plus d'ensembles de contrôles que ce que la console autorise actuellement, utilisez l'API CreateAssessmentFramework fournie par Audit Manager.

Pour spécifier les contrôles dans les ensembles de contrôles

1. Sous Nom de l'ensemble de contrôles, entrez un nom pour votre ensemble de contrôles.
2. Sous Ajouter un nouveau contrôle à l'ensemble de contrôles, Sélectionner le type de contrôle, utilisez la liste déroulante pour sélectionner l'un des deux types de contrôle : Contrôles standard ou Contrôles personnalisés. Les contrôles standard sont fournis par Audit Manager, et les contrôles personnalisés sont ceux que vous créez.
3. En fonction de l'option que vous avez sélectionnée à l'étape précédente, une liste de contrôles standard ou personnalisés s'affiche. Vous pouvez parcourir la liste ou effectuer une recherche en

saisissant le nom du contrôle, la conformité ou la balise. Sélectionnez un ou plusieurs contrôles et choisissez Ajouter à l'ensemble de contrôles pour les ajouter à l'ensemble de contrôles.

4. Dans la fenêtre contextuelle qui apparaît, choisissez Ajouter à l'ensemble de contrôles pour confirmer votre ajout.
5. Sous Vérifier les contrôles sélectionnés dans l'ensemble de contrôles, passez en revue les contrôles qui apparaissent dans la liste Contrôles sélectionnés. Pour ajouter d'autres contrôles à un ensemble de contrôles, répétez les étapes 2 à 4. Vous pouvez supprimer des contrôles indésirables de l'ensemble de contrôles en sélectionnant un ou plusieurs contrôles, puis en choisissant Supprimer le contrôle.
6. Pour ajouter un nouvel ensemble de contrôles au framework, choisissez Ajouter un ensemble de contrôles au bas de la page. Vous pouvez supprimer les ensembles de contrôles indésirables en choisissant Supprimer l'ensemble de contrôles.
7. Une fois que vous avez terminé l'ajout des ensembles de contrôles et des contrôles, choisissez Suivant.

Étape 3 : Examen et création du framework

Vérifiez les informations de votre framework. Pour modifier les informations d'une étape, choisissez Modifier.

Lorsque vous avez terminé, choisissez Créer un framework personnalisé.

Que puis-je faire ensuite ?

Après avoir créé votre nouveau framework personnalisé, vous pouvez créer une évaluation à partir de celui-ci. Pour de plus amples informations, veuillez consulter Création d'une évaluation.

Vous pouvez également créer un framework personnalisé à l'aide d'un framework existant. Pour de plus amples informations, veuillez consulter Personnalisation d'un framework existant.

Pour obtenir des instructions sur la façon de modifier votre framework personnalisé, consultez Modification d'un framework personnalisé.

Personnalisation d'un framework existant

Vous pouvez utiliser des frameworks personnalisés dans AWS Audit Manager pour organiser les contrôles en ensembles de contrôles de manière à répondre à vos besoins spécifiques. Au lieu de

créer un tout nouveau framework personnalisé, vous pouvez utiliser un framework existant comme point de départ et le personnaliser. Dans ce cas, le framework existant reste dans la bibliothèque de frameworks, et un nouveau framework personnalisé est créé avec vos paramètres personnalisés.

Vous pouvez sélectionner n'importe quel framework existant à personnaliser. Il peut s'agir d'un framework standard ou d'un framework personnalisé.

Dans la bibliothèque de frameworks, dans la liste déroulante Créer un framework personnalisé, choisissez Personnaliser le framework existant. Procédez comme suit pour personnaliser le framework.

Rubriques

- Étape 1 : Spécifier les détails du framework
- Étape 2 : Indiquer les contrôles pour ajouter des ensembles de contrôles
- Étape 3 : Examen et création du framework
- Que puis-je faire ensuite ?

Étape 1 : Spécifier les détails du framework

Tous les détails du framework, à l'exception des balises, sont repris du framework d'origine. Vérifiez et modifiez ces détails si nécessaire.

Pour spécifier les détails du framework

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Bibliothèque de frameworks.
3. Choisissez le framework que vous souhaitez personnaliser, et dans la bibliothèque de frameworks, dans la liste déroulante Créer un framework personnalisé, choisissez Personnaliser le framework existant.
4. Dans la fenêtre contextuelle qui apparaît, entrez le nom du nouveau framework personnalisé et choisissez Personnaliser.
5. Sous Détails du framework, passez en revue le nom, le type de conformité et la description de votre framework, puis modifiez-les selon vos besoins. Le type de conformité doit indiquer la norme de conformité ou la réglementation associée à votre framework. Vous pouvez utiliser ce mot clé pour rechercher votre framework.

6. Sous Balises, choisissez Ajouter une nouvelle balise pour associer une balise à votre framework. Vous pouvez indiquer une clé et une valeur pour chaque balise. La clé de balise est obligatoire et peut être utilisée comme critère de recherche lorsque vous recherchez ce framework dans la bibliothèque de frameworks. Pour plus d'informations sur les balises dans AWS Audit Manager, consultez Balisage de ressources AWS Audit Manager.
7. Choisissez Suivant.

Étape 2 : Indiquer les contrôles pour ajouter des ensembles de contrôles

Les ensembles de contrôles sont reportés à partir du framework d'origine. Personnalisez la configuration actuelle en ajoutant des contrôles supplémentaires ou en supprimant des contrôles existants selon les besoins.

> **Note**
>
> Lorsque vous utilisez la console AWS Audit Manager pour personnaliser un framework, vous pouvez ajouter jusqu'à 10 ensembles de contrôles pour chaque framework. Lorsque vous utilisez l'API Audit Manager pour créer un framework personnalisé, vous pouvez ajouter plus de 10 ensembles de contrôles. Pour ajouter plus d'ensembles de contrôles que ce que la console autorise actuellement, utilisez l'API CreateAssessmentFramework fournie par Audit Manager.

Pour spécifier les contrôles dans l'ensemble de contrôles

1. Sous Nom de l'ensemble de contrôles, personnalisez le nom de l'ensemble de contrôles selon vos besoins.
2. Sous Ajouter un nouveau contrôle à l'ensemble de contrôles, ajoutez un nouveau contrôle en utilisant la liste déroulante pour sélectionner l'un des deux types de contrôle : Contrôles standard ou Contrôles personnalisés.
3. En fonction de l'option que vous avez sélectionnée à l'étape précédente, une liste de contrôles standard ou personnalisés s'affiche. Vous pouvez parcourir cette liste ou effectuer une recherche en saisissant le nom du contrôle, la conformité ou la balise pour localiser les contrôles à ajouter. Sélectionnez un ou plusieurs contrôles et choisissez Ajouter à l'ensemble de contrôles pour les ajouter à cet ensemble de contrôles.
4. Dans la fenêtre contextuelle qui apparaît, choisissez Ajouter à l'ensemble de contrôles pour confirmer votre ajout.

5. Sous Vérifier les contrôles sélectionnés dans l'ensemble de contrôles, passez en revue les contrôles qui apparaissent dans la liste Contrôles sélectionnés. Pour ajouter d'autres contrôles à un ensemble de contrôles, répétez les étapes 2 à 4. Vous pouvez supprimer des contrôles indésirables de l'ensemble de contrôles en sélectionnant un ou plusieurs contrôles, puis en choisissant Supprimer le contrôle.
6. Pour ajouter un nouvel ensemble de contrôles au framework, choisissez Ajouter un ensemble de contrôles au bas de la page. Vous pouvez supprimer les ensembles de contrôles indésirables en choisissant Supprimer l'ensemble de contrôles.
7. Une fois que vous avez terminé l'ajout des ensembles de contrôles et des contrôles, choisissez Suivant.

Étape 3 : Examen et création du framework

Vérifiez les informations de votre framework. Pour modifier les informations d'une étape, choisissez Modifier.

Lorsque vous avez terminé, choisissez Créer un framework personnalisé.

Que puis-je faire ensuite ?

Après avoir créé votre nouveau framework personnalisé, vous pouvez créer une évaluation à partir de celui-ci. Pour de plus amples informations, veuillez consulter Création d'une évaluation.

Pour obtenir des instructions sur la façon de modifier votre framework personnalisé, consultez Modification d'un framework personnalisé.

Modification d'un framework personnalisé

Vous pouvez utiliser des frameworks personnalisés dans AWS Audit Manager pour organiser les contrôles en ensembles de contrôles de manière à répondre à vos besoins spécifiques. Vous pouvez utiliser la bibliothèque de frameworks pour rechercher et modifier un framework personnalisé en suivant ces étapes.

Rubriques

- Étape 1 : Modifier les détails du framework
- Étape 2 : Indiquer les contrôles dans l'ensemble de contrôles

- Étape 3. Vérifier et mettre à jour le framework

Étape 1 : Modifier les détails du framework

Commencez par examiner et modifier les détails du framework existant.

Modifier les détails du framework

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Bibliothèque de frameworks, puis l'onglet Créer un framework personnalisé.
3. Sélectionnez le framework que vous souhaitez modifier, choisissez Actions, puis Modifier.
   - Vous pouvez également ouvrir un framework personnalisé et choisir Actions, Modifier en haut à droite de la page de résumé de l'évaluation.
4. Sous Détails du framework, passez en revue le nom, le type de conformité et la description de votre framework, puis modifiez-les si nécessaire.
5. Choisissez Next (Suivant).

> **Tip**
>
> Pour modifier les balises d'un framework, ouvrez le framework et choisissez l'onglet Balises du framework. Vous pouvez y afficher et modifier les balises associées au framework.

Étape 2 : Indiquer les contrôles dans l'ensemble de contrôles

Passez ensuite en revue et modifiez les contrôles et les ensembles de contrôles du framework.

> **Note**
>
> Lorsque vous utilisez la console AWS Audit Manager pour modifier un framework personnalisé, vous pouvez ajouter jusqu'à 10 ensembles de contrôles pour chaque framework.
> Lorsque vous utilisez l'API Audit Manager pour modifier un framework personnalisé, vous pouvez ajouter plus de 10 ensembles de contrôles. Pour ajouter plus

d'ensembles de contrôles que ce que la console autorise actuellement, utilisez l'API UpdateAssessmentFramework fournie par Audit Manager.

Pour modifier des contrôles

1. Sous Nom de l'ensemble de contrôles, vérifiez et modifiez le nom de votre ensemble de contrôles selon vos besoins.
2. Sous Ajouter un nouveau contrôle à l'ensemble de contrôles, vous pouvez ajouter un contrôle. Utilisez la liste déroulante pour sélectionner l'un des deux types de contrôle : Contrôles standard ou Contrôles personnalisés.
3. En fonction de l'option que vous avez sélectionnée à l'étape précédente, une liste de contrôles standard ou personnalisés s'affiche dans un tableau. Vous pouvez parcourir la liste des ensembles de contrôles. Ou, vous pouvez effectuer une recherche en saisissant le nom du contrôle, la source de données, ou les balises pour localiser les contrôles que vous souhaitez ajouter. Sélectionnez un ou plusieurs contrôles et choisissez Ajouter à l'ensemble de contrôles pour les ajouter à cet ensemble de contrôles.
4. Dans la fenêtre contextuelle qui apparaît, choisissez Ajouter à l'ensemble de contrôles pour confirmer votre ajout.
5. Sous Vérifier les contrôles sélectionnés dans l'ensemble de contrôles, passez en revue et modifiez les contrôles qui apparaissent dans la liste Contrôles sélectionnés. Pour ajouter d'autres contrôles à un ensemble de contrôles, répétez les étapes 2 à 4. Supprimez des contrôles indésirables de l'ensemble de contrôles en sélectionnant un ou plusieurs contrôles, puis en choisissant Supprimer le contrôle.
6. Pour ajouter un nouvel ensemble de contrôles au framework, choisissez Ajouter un ensemble de contrôles au bas de la page. Supprimez les ensembles de contrôles indésirables en choisissant Supprimer l'ensemble de contrôles.
7. Une fois que vous avez terminé l'ajout des ensembles de contrôles et des contrôles, choisissez Suivant.

Étape 3. Vérifier et mettre à jour le framework

Vérifiez les informations de votre framework. Pour modifier les informations d'une étape, choisissez Modifier.

Lorsque vous avez terminé, sélectionnez Enregistrer les modifications.

Suppression d'un framework personnalisé

Vous pouvez utiliser la bibliothèque de frameworks pour rechercher et supprimer un framework personnalisé indésirable. Vous pouvez également consulter les frameworks personnalisés à l'aide de l'API Audit Manager ou de AWS Command Line Interface (AWS CLI).

> **Note**
>
> La suppression d'un framework personnalisé n'affecte pas les évaluations existantes créées à partir du framework avant sa suppression.

Audit Manager console

Pour supprimer un framework personnalisé (console)

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation de gauche, choisissez Bibliothèque de frameworks, puis l'onglet Frameworks personnalisés.
3. Sélectionnez le framework que vous souhaitez supprimer, choisissez Actions, puis Modifier.
   - Vous pouvez également ouvrir un framework personnalisé et choisir Actions, Supprimer en haut à droite de la page de résumé du framework.
4. Dans la fenêtre contextuelle, choisissez Supprimer pour confirmer la suppression.

AWS CLI

Pour supprimer un framework personnalisé (AWS CLI)

1. Identifiez d'abord le framework personnalisé que vous souhaitez supprimer. Pour ce faire, exécutez la commande list-assessment-frameworks et spécifiez `--framework-type` comme `Custom`.

   ```
   aws auditmanager list-assessment-frameworks --framework-type Custom
   ```

   La réponse renvoie une liste de frameworks personnalisés. Recherchez le framework personnalisé que vous souhaitez supprimer et prenez note de l'ID du framework.

2. Ensuite, exécutez la commande delete-assessment-framework et spécifiez le `--framework-id` du framework que vous souhaitez supprimer.

   Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations.

   ```
   aws auditmanager delete-assessment-framework --framework-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

Audit Manager API

Pour supprimer un framework personnalisé (API)

1. Utilisez la commande ListAssessmentFrameworks et spécifiez le frameworkType comme `Custom`. Pour la réponse, recherchez le framework personnalisé que vous souhaitez supprimer et prenez note de l'ID du framework.
2. Utilisez l'opération DeleteAssessmentFramework pour supprimer le framework. Dans la requête, utilisez le paramètre frameworkId pour spécifier le framework que vous souhaitez supprimer.

Pour plus d'informations sur ces opérations d'API, cliquez sur l'un des liens précédents dans le Guide de référence de l'API AWS Audit Manager. Il inclut des informations sur l'utilisation du fonctionnement et des paramètres dans l'un des SDK AWS spécifiques au langage.

Partage d'un framework personnalisé

Vous pouvez utiliser la fonctionnalité de partage de frameworks de AWS Audit Manager pour répliquer rapidement les frameworks personnalisés que vous créez. Vous pouvez partager vos frameworks personnalisés avec un autre Compte AWS, ou les répliquer dans une autre Région AWS dans votre propre compte. Le destinataire peut ensuite accéder à votre framework personnalisé et l'utiliser pour créer des évaluations. Il peut le faire sans avoir à répéter vos efforts de configuration pour ce framework.

Pour partager un framework personnalisé, vous devez créer une demande de partage. Le destinataire de la demande de partage dispose alors de 120 jours pour accepter ou refuser la demande. Lorsqu'il accepte la demande de partage, Audit Manager réplique le framework personnalisé partagé dans sa bibliothèque de frameworks. Outre la réplication du framework

personnalisé, Audit Manager reproduit également tous les ensembles de contrôles personnalisés et les contrôles personnalisés faisant partie de ce framework. Ces contrôles personnalisés sont ajoutés à la bibliothèque de contrôles du destinataire. Audit Manager ne réplique pas les frameworks ou les contrôles standard. Par défaut, ils sont disponibles dans tous les Comptes AWS et régions où Audit Manager est activé.

La fonctionnalité de partage de framework est disponible uniquement dans la version payante. Cependant, le partage d'un framework personnalisé et l'acceptation d'une demande de partage ne sont soumis à aucuns frais supplémentaires. Pour en savoir plus sur la tarification de AWS Audit Manager, veuillez consulter la page de tarification de AWS Audit Manager.

> **Important**
>
> Vous ne pouvez pas partager un framework personnalisé dérivé d'un framework standard si celui-ci est désigné comme non éligible au partage par AWS, sauf si vous avez obtenu l'autorisation de le faire auprès du propriétaire du framework standard. Pour savoir quels frameworks standard ne sont pas éligibles au partage et en savoir plus, consultez la section Éligibilité au partage des frameworks.

Les sections suivantes de ce guide décrivent les informations importantes que vous devez connaître sur le partage de frameworks. Elles fournissent également des instructions sur la manière dont vous pouvez partager vos frameworks personnalisés et répondre aux demandes de partage.

Rubriques

- Concepts et terminologie de partage de frameworks
- Envoi d'une demande de partage pour un framework personnalisé
- Réponse aux demandes de partage
- Suppression de demandes de partage

> **Tip**
>
> Si vous ne connaissez pas les frameworks personnalisés Audit Manager et ne savez pas comment les créer, vous pouvez en savoir plus sur la page Création d'un framework personnalisé de ce guide.

Concepts et terminologie de partage de frameworks

Si vous découvrez les concepts clés suivants, vous pourrez tirer le meilleur parti de la fonctionnalité de partage de frameworks personnalisés AWS Audit Manager.

Expéditeur

Il s'agit du créateur d'une demande de partage et du Compte AWS où se trouve le framework personnalisé. Les expéditeurs peuvent partager des frameworks personnalisés avec n'importe quel Compte AWS. Ou bien, ils répliquent un framework personnalisé sur n'importe quelle Région AWS prise en charge pour leur propre compte.

Destinataire

C'est le consommateur du framework partagé. Les destinataires peuvent accepter ou refuser une demande de partage émanant d'un expéditeur.

> **Note**
>
> Un destinataire peut être un compte administrateur délégué. Toutefois, vous ne pouvez pas partager de frameworks personnalisés avec un compte de gestion AWS Organizations.

Éligibilité du framework

Vous pouvez uniquement partager des frameworks personnalisés. Par défaut, les frameworks standard sont déjà présents dans l'ensemble des Comptes AWS et Régions AWS où AWS Audit Manager est activé. En outre, les frameworks personnalisés que vous partagez ne doivent pas contenir de données sensibles. Cela inclut les données présentes dans le framework lui-même, ses ensembles de contrôles et tous les contrôles personnalisés inclus dans le framework personnalisé.

> **Important**
>
> Certains des frameworks standard proposés par AWS Audit Manager contiennent du matériel protégé par des droits d'auteur soumis à des contrats de licence. Les frameworks personnalisés peuvent contenir du contenu dérivé de ces frameworks. Vous ne pouvez pas partager un framework personnalisé dérivé d'un framework standard si le framework

standard est désigné comme non éligible au partage par AWS, sauf si vous avez obtenu l'autorisation de le faire auprès du propriétaire du framework standard.
Pour savoir quels frameworks standard sont éligibles au partage, reportez-vous au tableau suivant.

Nom du framework standard	Versions personnalisées éligibles au partage
Essential Eight du Centre australien de cybersécurité (ACSC)	 Oui
Manuel de sécurité de l'information du Centre australien de cybersécurité (ACSC)	 Oui
Exemple de framework AWS Audit Manager	 Oui
Barrières de protection AWS Control Tower	 Oui
Framework des bonnes pratiques en matière d'IA générative AWS v1	 Oui
Gestionnaire de licences AWS	 Oui
Bonnes pratiques de sécurité de base AWS	 Oui

Nom du framework standard	Versions personnalisées éligibles au partage
Bonnes pratiques de fonctionnement pour AWS	 Oui
Framework AWS Well-Architected	 Oui
Centre canadien pour la cybersécurité - Medium	 Non
Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.2.0, niveau 1	 Non
Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.2.0, niveaux 1 et 2	 Non
Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.3.0, niveau 1	 Non
Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.3.0, niveaux 1 et 2	 Non
Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.4.0, niveau 1	 Non

Nom du framework standard	Versions personnalisées éligibles au partage
Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.4.0, niveaux 1 et 2	Non
Contrôles CIS v7.1 IG1	Oui
Contrôles CIS v8 IG1	Non
Référence modérée FedRAMP	Oui
RGPD	Oui
Loi Gramm-Leach-Bliley (GLBA)	Oui
GxP 21 CFR partie 11	Oui
Annexe 11 du GxP EU	Oui

Nom du framework standard	Versions personnalisées éligibles au partage
HIPAA Security Rule 2003	Oui
HIPAA Final Omnibus Security Rule 2013	Oui
ISO/IEC 27001:2013 Annexe A	Non
NIST 800-53 (Rev. 5) Low-Moderate-High	Oui
Framework de cybersécurité du NIST version 1.1	Oui
NIST SP 800-171 Rev. 2	Oui
PCI DSS v3.2.1	Non
PCI DSS v4.0	Non

Nom du framework standard	Versions personnalisées éligibles au partage
SOC 2	 Non

Demande de partage

Pour partager un framework personnalisé, vous devez créer une demande de partage. La demande de partage indique un destinataire et l'informe qu'un framework personnalisé est disponible. Les destinataires ont 120 jours pour répondre à une demande de partage en l'acceptant ou en la refusant. Si aucune action n'est entreprise dans les 120 jours, la demande de partage expire et le destinataire perd la possibilité d'ajouter le framework personnalisé à sa bibliothèque de frameworks. Les expéditeurs et les destinataires peuvent consulter les demandes de partage et y donner suite depuis la page des demandes de partage de la bibliothèque de frameworks.

Statut des demandes de partage

Les demandes de partage peuvent présenter les statuts suivants.

- Actif : cela indique qu'une demande de partage a été envoyée avec succès au destinataire et que sa réponse est en attente.
- Arrive à expiration : cela indique une demande de partage qui expirera dans les 30 prochains jours.
- Partagé : cela indique une demande de partage acceptée par le destinataire.
- Inactif : cela indique qu'une demande de partage a été révoquée, refusée ou a expiré avant que le destinataire n'agisse.
- Réplication : cela indique une demande de partage acceptée qui est répliquée dans la bibliothèque de frameworks du destinataire.
- Échec : cela indique qu'une demande de partage n'a pas été envoyée avec succès au destinataire.

Notifications de demande de partage

Audit Manager informe les destinataires lorsqu'ils reçoivent une demande de partage. Les destinataires et les expéditeurs reçoivent une notification lorsqu'une demande de partage expire dans les 30 prochains jours.

- Pour les destinataires, un point de notification bleu apparaît à côté des demandes reçues ayant le statut Actif ou Arrive à expiration. Le destinataire peut agir sur la notification en acceptant ou en refusant la demande de partage.
- Pour les destinataires, un point de notification bleu apparaît à côté des demandes reçues ayant le statut Arrive à expiration. La notification est classée lorsque le destinataire accepte ou refuse la demande de partage. Dans le cas contraire, elle est classée à l'expiration de la demande. En outre, l'expéditeur peut agir sur la notification en révoquant la demande de partage.

Propriété de l'expéditeur

Les expéditeurs conservent un accès complet aux frameworks personnalisés qu'ils partagent. Ils peuvent annuler les demandes de partage actives à tout moment en révoquant la demande de partage avant son expiration. Toutefois, une fois qu'un destinataire a accepté une demande de partage, l'expéditeur ne peut plus révoquer l'accès du destinataire à ce framework personnalisé. En effet, lorsque le destinataire accepte la demande, Audit Manager crée une copie indépendante du framework personnalisé dans la bibliothèque de frameworks du destinataire.

Outre la réplication du framework personnalisé de l'expéditeur, Audit Manager reproduit également tous les ensembles de contrôles personnalisés et les contrôles personnalisés faisant partie de ce framework. Toutefois, Audit Manager ne réplique aucune balise attachée au framework personnalisé.

Propriété du destinataire

Les destinataires ont un accès complet aux frameworks personnalisés qu'ils acceptent. Lorsque le destinataire accepte la demande, Audit Manager réplique le framework personnalisé dans l'onglet Frameworks personnalisés de sa bibliothèque de frameworks. Les destinataires peuvent ensuite gérer le framework personnalisé partagé de la même manière que n'importe quel autre framework personnalisé. Les destinataires peuvent partager les frameworks personnalisés qu'ils reçoivent d'autres expéditeurs. Les destinataires ne peuvent empêcher les expéditeurs d'envoyer des demandes de partage.

Expiration du framework partagé

Lorsqu'un expéditeur crée une demande de partage, Audit Manager configure la demande pour qu'elle expire au bout de 120 jours. Les destinataires peuvent accepter le framework partagé et

y accéder avant l'expiration de la demande. Si un destinataire ne l'accepte pas pendant cette période, la demande de partage expire. À partir de là, un enregistrement de la demande de partage expirée reste dans son historique. Les instantanés des frameworks partagés expirés sont archivés dans un compartiment S3 avec un TTL d'un an à des fins d'audit.

Les expéditeurs peuvent choisir de révoquer une demande de partage à tout moment avant son expiration.

Sauvegarde et stockage des données du framework partagé

Lorsque vous créez une demande de partage, Audit Manager stocke un instantané de votre framework personnalisé dans la région USA Est (Virginie du Nord)Région AWS. Audit Manager stocke également une sauvegarde du même instantané dans USA Ouest (Oregon)Région AWS.

Audit Manager supprime l'instantané et l'instantané de sauvegarde lorsque l'un des événements suivants se produit :

- L'expéditeur révoque la demande de partage.
- Le destinataire refuse la demande de partage.
- Le destinataire rencontre une erreur et n'accepte pas correctement la demande de partage.
- La demande de partage expire avant que le destinataire ne réponde à la demande.

Lorsqu'un expéditeur renvoie une demande de partage, l'instantané est remplacé par une version mise à jour correspondant à la dernière version du framework personnalisé.

Lorsqu'un destinataire accepte une demande de partage, l'instantané est répliqué dans son Compte AWS sous la Région AWS spécifiée dans la demande de partage.

Gestion des versions des frameworks partagés

Lorsque vous partagez un framework personnalisé, Audit Manager crée une copie indépendante de ce framework dans le Compte AWS et la région spécifiée. Cela signifie que vous devez garder à l'esprit les points suivants :

- Le framework partagé qu'un destinataire accepte est un instantané du framework au moment de la création de la demande de partage. Si vous mettez à jour le framework personnalisé d'origine après avoir envoyé une demande de partage, celle-ci n'est pas automatiquement mise à jour. Pour partager la dernière version du framework mis à jour, vous pouvez renvoyer la demande de partage. La date d'expiration de ce nouvel instantané est de 120 jours à compter de la date du nouveau partage.

- Lorsque vous partagez un framework personnalisé avec un autre Compte AWS, puis que vous le supprimez de votre bibliothèque de frameworks, le framework personnalisé partagé reste dans la bibliothèque de frameworks du destinataire.
- Lorsque vous partagez un framework personnalisé avec une autre Région AWS depuis votre compte, puis que vous supprimez ce framework personnalisé dans la première Région AWS, le framework personnalisé reste dans la deuxième région.
- Lorsque vous supprimez un framework personnalisé partagé après l'avoir accepté, tous les contrôles personnalisés répliqués dans le cadre du framework personnalisé restent dans votre bibliothèque de contrôles.

Envoi d'une demande de partage pour un framework personnalisé

Ce tutoriel explique comment partager vos frameworks personnalisés entre Comptes AWS et Régions AWS.

Lorsque vous partagez un framework personnalisé, Audit Manager crée un instantané de votre framework et envoie une demande de partage au destinataire. Le destinataire dispose de 120 jours pour accepter le framework partagé. Lorsqu'il accepte la demande de partage, Audit Manager réplique le framework personnalisé partagé dans sa bibliothèque de frameworks dans la Région AWS spécifiée. Si vous souhaitez répliquer un framework personnalisé dans une autre région sous votre propre compte, utilisez le tutoriel suivant et entrez votre propre identifiant de Compte AWS comme identifiant de compte du destinataire.

Ce tutoriel contient les étapes suivantes :

1. Sélectionner un framework à partager : parcourez la bibliothèque de frameworks pour trouver le framework personnalisé que vous souhaitez partager.
2. Envoyer une demande de partage : spécifiez un destinataire et envoyez-lui une demande de partage pour le framework personnalisé.
3. Afficher les demandes envoyées : consultez l'historique de vos demandes de partage et vérifiez le statut de vos demandes envoyées.
4. (Facultatif) Révoquer la demande de partage : révoquez la demande de partage avant son expiration.

Prérequis

Avant de commencer ce tutoriel, vérifiez d'abord que vous remplissez les conditions suivantes :

- Vous connaissez les concepts et la terminologie de partage de frameworks Audit Manager.
- Le framework personnalisé que vous souhaitez partager est éligible au partage et existe dans la bibliothèque de frameworks de votre environnement AWS Audit Manager.
- Le destinataire a déjà activé AWS Audit Manager dans la Région AWS où vous souhaitez partager le framework personnalisé.
- Le destinataire n'est pas un compte de gestion AWS Organizations.

> **Tip**
>
> Avant de commencer, notez l'identifiant de Compte AWS avec lequel vous souhaitez partager votre framework personnalisé. Il peut s'agir de votre propre identifiant de compte, si votre objectif est de reproduire le framework sur une autre Région AWS avec votre compte. Vous aurez besoin de ces informations à l'étape 2 de ce tutoriel.

> **Important**
>
> Ne partagez pas de frameworks personnalisés contenant des données sensibles. Cela inclut les données présentes dans le framework lui-même, ses ensembles de contrôles et tous les contrôles personnalisés qui composent le framework personnalisé. Pour plus d'informations, consultez Éligibilité du framework.

Étape 1 : Identifier le framework personnalisé que vous souhaitez partager

Commencez par identifier le framework personnalisé que vous souhaitez partager. Vous pouvez consulter tous les frameworks personnalisés disponibles sur la page Bibliothèque de frameworks d'Audit Manager.

Pour consulter vos frameworks personnalisés disponibles

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Bibliothèque de frameworks.

3. Choisissez l'onglet Frameworks personnalisés. Cela affiche une liste de vos frameworks personnalisés disponibles. Vous pouvez choisir un nom de framework pour afficher les détails de ce framework personnalisé.

Étape 2 : Envoyer une demande de partage

Ensuite, spécifiez un destinataire et envoyez-lui une demande de partage pour le framework personnalisé. La destinataire dispose de 120 jours pour répondre à cette demande de partage avant qu'elle n'expire.

Pour envoyer une demande de partage

1. Dans l'onglet Frameworks personnalisés de la bibliothèque de frameworks, choisissez le nom d'un framework pour ouvrir la page de détails. À partir de là, choisissez Actions, puis sélectionnez Partager le framework personnalisé.
   - Vous pouvez également sélectionner un framework personnalisé dans la liste de la bibliothèque de frameworks, choisir Actions, puis Partager le framework personnalisé. En fonction de la taille du framework personnalisé, cette méthode peut prendre quelques secondes, le temps qu'Audit Manager prépare la demande de partage.
2. Consultez l'avis qui s'affiche dans la boîte de dialogue.
   - Si vous ne savez pas si vous pouvez partager votre framework personnalisé, consultez Éligibilité du framework pour obtenir des conseils supplémentaires.
   - Si votre framework comporte des contrôles qui utilisent des règles personnalisées AWS Config comme source de données, nous vous recommandons de contacter le destinataire pour le lui faire savoir. Le destinataire peut ensuite créer et activer les mêmes règles AWS Config dans son instance de AWS Config. Pour de plus amples informations, veuillez consulter Mon cadre partagé comporte des contrôles qui utilisent des règles AWS Config personnalisées comme source de données. Le destinataire peut-il collecter des preuves pour ces contrôles ?.
3. Saisissez **`agree`**, puis choisissez Accepter pour continuer.
4. Sur l'écran suivant, procédez comme suit :
   - Dans Compte AWS, saisissez l'identifiant de compte du destinataire. Il peut s'agir de votre propre ID de compte.
   - Dans Région AWS, sélectionnez la région du destinataire dans la liste déroulante.

- (Facultatif) Sous Message au destinataire, entrez un commentaire facultatif concernant le framework personnalisé que vous partagez.
- Sous Détails du framework personnalisé, passez en revue les détails pour confirmer que vous souhaitez partager ce framework.

5. Choisissez Partager.

> **Note**
>
> Gardez les points suivants à l'esprit :
>
> - Lorsque vous partagez un framework personnalisé avec un autre Compte AWS, le framework est répliqué uniquement vers la Région AWS spécifiée. Après avoir accepté la demande de partage, le destinataire peut ensuite reproduire le framework dans toutes les régions selon ses besoins.
> - Lorsque vous partagez des frameworks personnalisés entre Régions AWS, le traitement des actions de demande de partage peut prendre jusqu'à 10 minutes. Après avoir envoyé une demande de partage entre régions, nous vous recommandons de revenir ultérieurement vérifier que votre demande de partage a bien été envoyée.
> - Lorsque vous envoyez une demande de partage, Audit Manager prend un instantané du framework personnalisé au moment de la création de la demande de partage. Si vous mettez à jour le framework personnalisé d'origine après avoir envoyé une demande de partage, la demande n'est pas automatiquement mise à jour. Pour partager la dernière version d'un framework mis à jour, vous pouvez renvoyer la demande de partage. La date d'expiration de ce nouvel instantané est de 120 jours à compter de la date du nouveau partage.

Étape 3 : Afficher vos demandes envoyées

Vous pouvez sélectionner l'onglet Demandes envoyées pour afficher la liste de toutes les demandes de partage que vous avez envoyées. Vous pouvez filtrer cette liste selon vos besoins. Par exemple, vous pouvez appliquer des filtres pour afficher uniquement les demandes qui expirent dans les 30 prochains jours.

Pour consulter et filtrer les demandes que vous avez envoyées

1. Dans le panneau de navigation, sélectionnez Demandes de partage.

2. Choisissez l'onglet Demandes envoyées.
3. (Facultatif) Appliquez des filtres pour affiner les demandes envoyées qui sont visibles. Pour ce faire, recherchez la liste déroulante Tous les statuts et remplacez le filtre par l'un des filtres suivants.

   - Actif : ce filtre affiche les demandes de partage en attente d'une réponse du destinataire.
   - Partagé : ce filtre affiche les demandes de partage acceptées par le destinataire. Le framework personnalisé partagé existe désormais dans la bibliothèque de frameworks du destinataire.
   - Inactif : cela indique les demandes de partage qui ont été révoquées, refusées ou ont expiré avant que le destinataire n'agisse. Choisissez le mot Inactif pour afficher plus de détails.
   - Arrive à expiration : ce filtre affiche les demandes de partage qui expirent dans les 30 prochains jours.
   - Échec : ce filtre affiche les demandes de partage qui n'ont pas été correctement envoyées au destinataire. Choisissez le mot Échec pour afficher plus de détails.

> **Note**
>
> Le traitement d'une demande de partage peut prendre jusqu'à 15 minutes. Par conséquent, si une erreur se produit lors de l'envoi de votre demande de partage au destinataire, le statut Échec risque de ne pas s'afficher immédiatement. Nous vous recommandons de revenir ultérieurement vérifier que votre demande de partage a bien été envoyée.
> Pour plus d'informations sur la procédure à suivre en cas d'erreur, consultez la section Résolution des problèmes liés aux demandes de partage.

Étape 4 (Facultatif) : Révoquer la demande de partage

Si vous devez annuler une demande de partage active avant son expiration, vous pouvez la révoquer à tout moment. Cette étape est facultative. Si vous ne faites rien, le destinataire ne sera plus en mesure d'accepter la demande de partage après la date d'expiration.

Pour révoquer une demande de partage

1. Dans le panneau de navigation, sélectionnez Demandes de partage.
2. Choisissez l'onglet Demandes envoyées.
3. Sélectionnez le framework que vous souhaitez révoquer, puis Révoquer la demande.

4. Dans la fenêtre contextuelle qui s'affiche, choisissez Révoquer.

> **Note**
>
> Vous ne pouvez révoquer l'accès qu'aux demandes de partage dont le statut est Actif ou Arrive à expiration. Une fois qu'un destinataire a accepté une demande de partage, vous ne pouvez plus révoquer l'accès du destinataire à ce framework personnalisé. Cela est dû au fait qu'une copie du framework personnalisé existe désormais dans la bibliothèque de frameworks du destinataire.
>
> Lorsque vous partagez des frameworks entre Régions AWS, le traitement des actions de demande de partage peut prendre jusqu'à 10 minutes. Après avoir révoqué une demande de partage entre régions, nous vous recommandons de revenir ultérieurement vérifier que votre demande de partage a bien été révoquée.

Renvoi d'une demande de partage pour un framework mis à jour

Vous pouvez envoyer une demande de partage pour un framework personnalisé, puis mettre à jour le même framework par la suite. Dans ce cas, la demande de partage n'est pas automatiquement mise à jour pour refléter la dernière version du framework. Toutefois, si le statut est Actif, Partagé ou Arrive à expiration, vous pouvez mettre à jour une demande de partage existante. Pour ce faire, vous devez renvoyer une nouvelle demande de partage avec les mêmes informations que la demande existante. Dans la nouvelle demande de partage, incluez le même identifiant de framework personnalisé, le même identifiant de compte destinataire et la même Région AWS destinataire. Vous pouvez également ajouter un nouveau commentaire à la nouvelle demande de partage.

Gardez à l'esprit les points suivants lorsque vous renvoyez une demande de partage :

- Pour que la mise à jour soit réussie, la nouvelle demande doit concerner le même identifiant de framework personnalisé. Elle doit également spécifier le même numéro de compte destinataire et la même région que pour la demande existante.
- Si le nom du framework personnalisé a changé, la demande de partage mise à jour affiche le nom le plus récent.
- Si vous fournissez un nouveau commentaire, la demande de partage mise à jour affiche le dernier commentaire.
- Lorsque vous renvoyez une demande de partage, la date d'expiration est prolongée de six mois.

Pour renvoyer une demande de partage pour un framework mis à jour

1. Dans l'onglet Frameworks personnalisés de la bibliothèque de frameworks, choisissez le nom du framework que vous souhaitez partager. Cette action ouvre la page détaillée du framework. À partir de là, choisissez Actions, puis sélectionnez Partager le framework personnalisé.

   - Vous pouvez également sélectionner le framework personnalisé dans la liste de la bibliothèque de frameworks, choisir Actions, puis Partager le framework personnalisé. En fonction de la taille du framework personnalisé, cette méthode peut prendre quelques secondes, le temps qu'Audit Manager prépare la demande de partage.

2. Consultez l'avis qui s'affiche dans la boîte de dialogue, entrez **`agree`**, puis choisissez Accepter pour continuer.
3. Sur l'écran suivant, procédez comme suit :

   - Sous Compte AWS, entrez le même identifiant de compte que celui que vous avez spécifié dans la demande de partage existante.
   - Sous Région AWS, entrez la même région que celle que vous avez spécifié dans la demande de partage existante.
   - (Facultatif) Sous Message au destinataire, entrez un commentaire facultatif concernant le framework personnalisé mis à jour.
   - Sous Détails du framework personnalisé, passez en revue les détails pour confirmer que vous souhaitez renvoyer la demande de partage.

4. Choisissez Partager pour renvoyer et mettre à jour la demande de partage.

Résoudre les problèmes liés aux demandes

Pour trouver des solutions aux problèmes que vous pourriez rencontrer lors du partage d'un framework personnalisé, consultez Résolution des problèmes liés au partage de cadre dans la section Résolution des problèmes de ce guide.

Réponse aux demandes de partage

Ce tutoriel décrit les actions à effectuer lorsque vous recevez une demande de partage pour un framework personnalisé. Audit Manager vous informe lorsque vous recevez une demande de partage. Vous recevez aussi une notification lorsqu'une demande de partage expire dans les 30 prochains jours.

Ce tutoriel contient les étapes suivantes :

1. Consulter vos notifications de demande de partage : consultez la liste des demandes de partage actives qui expirent bientôt.
2. Agir sur la demande de partage : acceptez ou refusez la demande de partage pour le framework personnalisé.
3. Afficher les demandes de partage que vous avez reçues d'autres personnes : consultez l'historique de vos demandes de partage.

Prérequis

Avant de commencer, nous vous recommandons d'en apprendre plus sur les concepts et la terminologie de partage de framework Audit Manager.

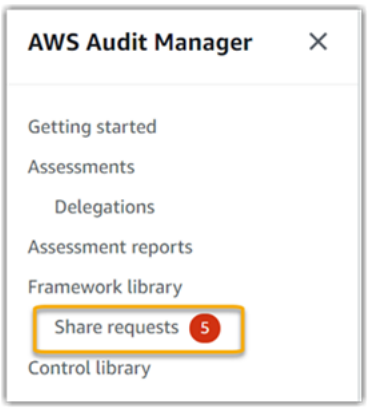
Étape 1 : Vérifier les notifications de demande que vous avez reçues

Commencez par vérifier vos notifications de demande de partage. L'onglet Demandes reçues affiche la liste des demandes de partage que vous avez reçues d'autres Comptes AWS. Les demandes en attente de réponse apparaissent avec un point bleu. Vous pouvez également filtrer cette vue pour n'afficher que les demandes qui expirent dans les 30 prochains jours.

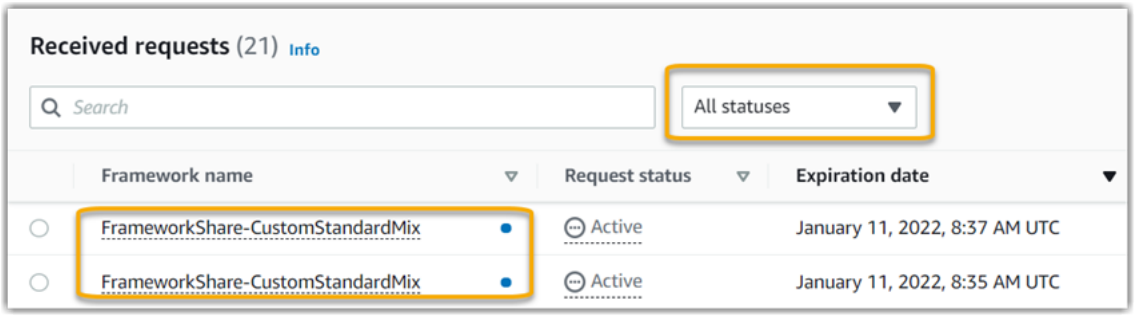
Pour consulter les demandes reçues

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Si vous avez reçu une notification de demande de partage, Audit Manager affiche un point rouge à côté de l'icône du menu de navigation.

3. Développez le volet de navigation et regardez à côté de Demandes de partage. Un badge de notification indique le nombre de demandes de partage qui nécessitent votre attention.



4. Choisissez Demandes de partage. Par défaut, cette page s'ouvre dans l'onglet Demandes reçues.
5. Identifiez les demandes de partage qui nécessitent une action de votre part en recherchant les éléments marqués d'un point bleu.



6. (Facultatif) Pour afficher uniquement les demandes qui expireront dans les 30 prochains jours, recherchez la liste déroulante Tous les statuts et sélectionnez Arrive à expiration.

Étape 2 : Agir sur une demande

Pour supprimer le point de notification bleu, vous devez agir en acceptant ou en refusant la demande de partage.

> **Note**
>
> Le traitement des actions de demande de partage peut prendre jusqu'à 10 minutes lors d'un partage de framework entre Régions AWS. Après avoir accepté une demande de partage entre régions, nous vous recommandons de revenir ultérieurement vérifier que votre demande de partage a bien été acceptée ou refusée.

Accepter un framework partagé

Lorsque vous acceptez une demande de partage, Audit Manager réplique un instantané du framework d'origine dans l'onglet Frameworks personnalisés de votre bibliothèque de frameworks. Audit Manager réplique et chiffre le nouveau framework personnalisé à l'aide de la clé KMS que vous avez spécifiée dans vos Paramètres Audit Manager.

Pour accepter une demande de partage

1. Ouvrez la page Demandes de partage et assurez-vous de consulter l'onglet Demandes reçues.
2. (Facultatif) Sélectionnez Actif ou Arrive à expiration dans la liste déroulante des filtres.
3. (Facultatif) Choisissez un nom de framework pour afficher les détails de la demande de partage. Cela inclut des informations comme la description du framework, le nombre de contrôles présents dans le framework et le message de l'expéditeur.
4. Sélectionnez la demande de partage que vous souhaitez accepter, choisissez Actions, puis Accepter.

Une fois que vous avez accepté une demande de partage, le statut passe à Réplication, tandis que le framework personnalisé partagé est ajouté à votre bibliothèque de frameworks. Si le framework contient des contrôles personnalisés, ces contrôles sont ajoutés à votre bibliothèque de contrôles pour le moment.

Une fois le framework répliqué, le statut devient Partagé. Une bannière de réussite vous indique que le framework personnalisé est prêt à être utilisé.

> **Tip**
>
> Lorsque vous acceptez un framework personnalisé, il est répliqué uniquement sur dans votre Région AWS actuelle. Vous souhaiterez peut-être que le nouveau framework partagé soit disponible dans toutes les régions de votre Compte AWS. Si tel est le cas, après avoir accepté la demande de partage, vous pouvez partager le framework avec d'autres régions sous votre compte selon vos besoins.

Refuser un partage de framework

Lorsque vous refusez une demande de partage, Audit Manager n'ajoute pas ce framework personnalisé à votre bibliothèque de frameworks. Cependant, un enregistrement de la demande de partage refusée reste dans l'onglet Demandes reçues, avec le statut Inactif.

Pour refuser une demande de partage

1. Ouvrez la page Demandes de partage et assurez-vous de consulter l'onglet Demandes reçues.
2. (Facultatif) Sélectionnez Actif ou Arrive à expiration dans la liste déroulante des filtres.
3. (Facultatif) Choisissez un nom de framework pour afficher les détails de la demande de partage. Cela inclut des informations comme la description du framework, le nombre de contrôles présents dans le framework et le message de l'expéditeur.
4. Sélectionnez la demande de partage que vous souhaitez refuser, choisissez Actions, puis Refuser.
5. Dans la boîte de dialogue qui s'affiche, choisissez Refuser pour confirmer votre choix.

> **Tip**
>
> Si vous changez d'avis et souhaitez accéder à un framework partagé après avoir refusé, demandez à l'expéditeur de vous envoyer une nouvelle demande de partage.

Étape 3 : Afficher l'historique des demandes que vous avez reçues

Après avoir accepté ou refusé un framework partagé, vous pouvez revenir à la page Demandes de partage pour consulter l'historique de vos demandes de partage. Vous pouvez filtrer cette liste selon vos besoins. Par exemple, vous pouvez appliquer des filtres pour afficher uniquement les demandes que vous avez acceptées.

Pour consulter l'historique de vos demandes de partage

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation de gauche, sélectionnez Demandes de partage.
3. Choisissez l'onglet Demandes reçues.
4. Recherchez la liste déroulante Tous les statuts, puis sélectionnez l'un des filtres suivants.

- Actif : ce filtre affiche les demandes de partage que vous n'avez pas encore acceptées ou refusées.
- Arrive à expiration : ce filtre affiche les demandes de partage qui expirent dans les 30 prochains jours.
- Partagé : ce filtre affiche les demandes de partage que vous avez acceptées. Le framework partagé est désormais disponible dans votre bibliothèque de frameworks.
- Inactif : ce filtre affiche les demandes de partage qui ont été refusées ou ont expiré.
- Échec : ce filtre affiche les demandes de partage qui n'ont pas été correctement envoyées. Choisissez le mot Échec pour afficher plus de détails.

Que puis-je faire ensuite ?

Une fois que vous avez accepté un framework personnalisé partagé, vous pouvez le trouver dans l'onglet Frameworks personnalisés de la bibliothèque du frameworks. Vous pouvez désormais utiliser ce framework pour créer une évaluation. Pour en savoir plus, veuillez consulter Création d'une évaluation. Pour obtenir des instructions sur la façon de modifier votre nouveau framework personnalisé, consultez Modifier un framework personnalisé.

Suppression de demandes de partage

Vous pouvez supprimer les demandes de partage qui ne sont plus souhaitées ou dont vous n'avez plus besoin.

> **Note**
>
> Vous ne pouvez pas supprimer les demandes de partage dont le statut est Actif ou Réplication.
> Lorsque vous supprimez une demande de partage, seule la demande elle-même est supprimée. Le framework partagé lui-même reste dans votre bibliothèque de frameworks.

Pour supprimer demande de partage

1. Dans le panneau de navigation, sélectionnez Demandes de partage.
2. Choisissez l'onglet Demandes envoyées ou Demandes reçues.
3. Sélectionnez le framework que vous ne souhaitez plus, puis choisissez Supprimer.

4. Dans la fenêtre contextuelle qui s'affiche, choisissez Supprimer.

Frameworks pris en charge dans AWS Audit Manager

AWS Audit Manager fournit les frameworks standard suivants. Ces frameworks prédéfinis sont basés sur les bonnes pratiques AWS relatives aux différentes normes et réglementations de conformité. Vous pouvez utiliser ces frameworks pour vous aider à préparer votre audit.

Rubriques

- Essential Eight du Centre australien de cybersécurité (ACSC)
- Manuel de sécurité de l'information du Centre australien de cybersécurité (ACSC)
- Exemple de framework AWS Audit Manager
- Barrières de protection AWS Control Tower
- Framework des bonnes pratiques en matière d'IA générative AWS v1
- AWS License Manager
- AWSBonnes pratiques de sécurité de base
- Bonnes pratiques de fonctionnement pour AWS
- AWS Well-Architected
- Centre canadien pour la cybersécurité - Profil de contrôle de cloud Medium
- Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.2.0
- Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.3.0
- Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.4.0
- Groupe 1 de mise en œuvre des Contrôles CIS v7.1
- Groupe 1 de mise en œuvre des contrôles CIS v8
- Référence modérée FedRAMP
- Règlement général sur la protection des données (RGPD)
- Loi Gramm-Leach-Bliley
- GxP 21 CFR partie 11
- Annexe 11 du GxP EU
- Règle de sécurité Health Insurance Portability and Accountability Act (HIPAA) de 2003
- Health Insurance Portability and Accountability Act (HIPAA) Final Omnibus Security Rule 2013
- ISO/IEC 27001:2013 Annexe A

- NIST 800-53 (Rev. 5) Low-Moderate-High
- Framework de cybersécurité du NIST version 1.1
- NIST SP 800-171 (Rev. 2)
- PCI DSS V3.2.1
- PCI DSS V4.0
- SOC 2

Essential Eight du Centre australien de cybersécurité (ACSC)

Pour vous aider à préparer votre audit, AWS Audit Manager fournit un framework standard prédéfini qui structure et automatise les évaluations pour le framework Essential Eight.

Rubriques

- Qu'est-ce que l'Essential Eight de l''Australian Cyber Security Centre (ACSC) ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources supplémentaires Essential Eight

Qu'est-ce que l'Essential Eight de l''Australian Cyber Security Centre (ACSC) ?

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

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

Utiliser ce framework pour faciliter la préparation de votre audit

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

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

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
Essential Eight	7	1	8	• AWS Config • AWS Security Hub

> **Tip**
>
> Pour consulter les règles AWS Config utilisées comme mappages de sources de données dans ce framework standard, téléchargez le fichier AuditManager_ConfigDataSourceMappings_EssentialEight.zip.

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

Vous trouverez le framework Essential Eight sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework Essential Eight. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation. Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources supplémentaires Essential Eight

- ACSC Essential Eight

Manuel de sécurité de l'information du Centre australien de cybersécurité (ACSC)

Pour vous aider à préparer votre audit, AWS Audit Manager fournit un framework standard prédéfini qui structure et automatise les évaluations pour le framework du Manuel de sécurité de l'information ACSC.

Rubriques

- Qu'est-ce que le Manuel de sécurité de l'information du Centre australien de cybersécurité (ACSC) ?
- Utiliser ce framework pour faciliter la préparation de votre audit

- Ressources supplémentaires sur le Manuel de sécurité de l'information ACSC

Qu'est-ce que le Manuel de sécurité de l'information du Centre australien de cybersécurité (ACSC) ?

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

Utiliser ce framework pour faciliter la préparation de votre audit

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

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

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
Manuel de sécurité de l'information ACSC	45	396	22	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Pour consulter les règles AWS Config utilisées comme mappages de sources de données dans ce framework standard, téléchargez le fichier AuditManager_ConfigDataSourceMappings_ACSC-Information-Security-Manual.zip.

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

Vous trouverez le framework du manuel de sécurité de l'information de l'ACSC sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework du manuel de sécurité de l'information de l'ACSC. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou

UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation. Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources supplémentaires sur le Manuel de sécurité de l'information ACSC

- Manuel de sécurité de l'information ACSC

Exemple de framework AWS Audit Manager

AWS Audit Manager fournit un framework type pour vous aider à démarrer la préparation de votre audit.

Rubriques

- Qu'est-ce que le Framework type AWS Audit Manager ?
- Utiliser ce framework pour faciliter la préparation de votre audit

Qu'est-ce que le Framework type AWS Audit Manager ?

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

Utiliser ce framework pour faciliter la préparation de votre audit

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

En utilisant le Framework type AWS Audit Manager comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des preuves pertinentes pour votre audit. Après

avoir créé une évaluation, Audit Manager commence à évaluer vos ressources AWS. Pour ce faire, il se base sur les contrôles définis dans le framework. Ensuite, il recueille les preuves pertinentes, puis les associe aux contrôles de votre évaluation.

Les détails du framework type AWS Audit Manager sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
Exemple de framework AWS Audit Manager	4	1	3	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework type AWS Audit Manager. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Barrières de protection AWS Control Tower

AWS Audit Manager fournit un framework de barrières de protection AWS Control Tower pour vous aider à préparer votre audit.

Rubriques

- Qu'est-ce qu'AWS Control Tower ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources AWS Control Tower supplémentaires

Qu'est-ce qu'AWS Control Tower ?

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

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

Le framework de barrières de protection AWS Control Tower contient tous les AWS Config Rules basés sur des barrières de protection de AWS Control Tower.

Utiliser ce framework pour faciliter la préparation de votre audit

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

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des preuves pertinentes pour votre audit AWS Control Tower. Après avoir créé une évaluation, Audit Manager commence à évaluer vos ressources AWS. Pour ce faire, il se

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

Les détails du framework de barrières de protection AWS Control Tower sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
Barrières de protection AWS Control Tower	14	0	5	AWS Config

> **Tip**
>
> Pour consulter les règles AWS Config utilisées comme mappages de sources de données dans ce framework standard, téléchargez le fichier AuditManager_ConfigDataSourceMappings_ControlTowerGuardrails.zip.

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

Vous trouverez le framework de barrières de protection AWS Control Tower sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer ou mettre à jour une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne

peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences des barrières de protection AWS Control Tower. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources AWS Control Tower supplémentaires

- Page des services AWS Control Tower
- Guide de l'utilisateur AWS Control Tower

Framework des bonnes pratiques en matière d'IA générative AWS v1

AWS Audit Manager fournit un framework standard prédéfini pour vous aider à mieux comprendre comment votre implémentation d'IA générative sur Amazon Bedrock fonctionne par rapport aux bonnes pratiques recommandées AWS.

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

Rubriques

- Que sont les bonnes pratiques AWS en matière d'IA générative pour Amazon Bedrock ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Vérification manuelle des invites dans Amazon Bedrock
- Ressources supplémentaires

Que sont les bonnes pratiques AWS en matière d'IA générative pour Amazon Bedrock ?

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

AWS s'engage à vous fournir les outils et les conseils nécessaires pour créer et gérer des applications de manière responsable. Pour vous aider à atteindre cet objectif, Audit Manager s'est associé à Amazon Bedrock pour créer le framework des bonnes pratiques d'IA générative AWS v1. Ce framework vous fournit un outil spécialement conçu pour surveiller et améliorer la gouvernance de vos projets d'IA générative sur Amazon Bedrock. Vous pouvez utiliser les bonnes pratiques de ce framework pour renforcer le contrôle et la visibilité de l'utilisation de votre modèle et rester informé du comportement de celui-ci.

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

1. Responsable : Élaborer et respecter des directives éthiques pour le déploiement et l'utilisation de modèles d'IA générative
2. Sûr : Établir des paramètres clairs et des limites éthiques pour empêcher la production de résultats nocifs ou problématiques
3. Équitable : Considérer et respecter l'impact d'un système d'IA sur les différentes sous-populations d'utilisateurs
4. Durable : Viser une plus grande efficacité et des sources d'énergie plus durables
5. Résilience : Maintenir les mécanismes d'intégrité et de disponibilité pour garantir le fonctionnement fiable d'un système d'IA
6. Confidentialité : S'assurer que les données sensibles sont protégées contre le vol et la divulgation

7. Précision : Créer des systèmes d'IA précis, fiables et robustes
8. Sécurisé : Empêcher l'accès non autorisé aux systèmes d'IA générative

Exemple

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

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

Utiliser ce framework pour faciliter la préparation de votre audit

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

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

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des preuves qui vous aideront à contrôler le respect des politiques prévues. Après avoir créé une évaluation, Audit Manager commence à évaluer vos ressources AWS. Pour ce faire, il se base sur les contrôles définis dans le framework AWS des bonnes pratiques en matière d'IA générative. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des

résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre d'ensembles de contrôles	Nombre de contrôles automatisés	Nombre de contrôles manuels	Services AWS dans le champ d'application
Framework des bonnes pratiques en matière d'IA générative AWS v1	8	34 entièrement automatisés 18 partiellement automatisés	58	• Amazon Bedrock • Amazon CloudWatch • Amazon S3 • AWS Backup • AWS CloudTrail • AWS Config • AWS Identity and Access Management

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

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation. Pour des instructions sur la façon d'effectuer une copie modifiable de ce framework afin de répondre à vos besoins spécifiques, consultez Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Vérification manuelle des invites dans Amazon Bedrock

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

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

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

Après avoir créé votre liste d'invites, testez chacune d'elles à l'aide de l'opération InvokeModel fournie par Amazon Bedrock. Vous pouvez ensuite collecter les réponses du modèle à ces invites et télécharger ces données sous forme de preuves manuelles dans votre évaluation Audit Manager.

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

1. Requête HTTP

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

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

2. AWS CLI

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

L'exemple suivant montre comment générer du texte avec la CLI AWS à l'aide de l'invite *« story of two dogs »* et du modèle *Anthropic Claude V2*. L'exemple renvoie jusqu'à 3*00* jetons dans la réponse et enregistre la réponse dans le fichier *invoke-model-output.txt* :

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

3. Vérification automatique

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

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

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

    const prompt = "Hello";
    const maxTokenCount = 512;
```

```
    const stopSequences = [];
    const temperature = 0.5;
    const topP = 0.5;

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

    var bedrockRuntime = new AWS.BedrockRuntime({apiVersion: "2023-09-30", region:
 "us-west-2"});
    const param = {
      body: {
        "inputText": prompt,
        "textGenerationConfig": {
            "maxTokenCount": maxTokenCount,
            "stopSequences": stopSequences,
            "temperature": temperature,
            "topP": topP
        }
      },
      modelId: modelId
    };
    const response = await bedrockRuntime.invokeModel(param);
    return "Successfully completed Bedrock::Invoke.";
};
```

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

Invites types

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

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

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

Pour tester les informations personnelles dans les réponses du modèle

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

Pour tester la présence de blasphèmes dans les réponses du modèle

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

Ressources supplémentaires

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

AWS License Manager

AWS Audit Manager fournit un framework AWS License Manager pour vous aider à préparer votre audit.

Rubriques

- Qu'est-ce qu'AWS License Manager ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources AWS License Manager supplémentaires

Qu'est-ce qu'AWS License Manager ?

Avec AWS License Manager, vous pouvez ainsi gérer vos licences logicielles auprès de différents fournisseurs de logiciels (tels que Microsoft, SAP, Oracle ou IBM) de manière centralisée dans les environnements AWS locaux et sur site. Le fait de disposer de toutes vos licences logicielles au même endroit permet un meilleur contrôle et une meilleure visibilité et vous aide potentiellement

à limiter les excédents de licences et à réduire le risque de non-conformité et de problèmes de signalement erronés.

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

Utiliser ce framework pour faciliter la préparation de votre audit

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

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

Les détails du framework AWS License Manager sont les suivants :

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

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework AWS License Manager. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources AWS License Manager supplémentaires

Liens vers le Gestionnaire de licences

- Page des services AWS License Manager
- Guide de l'utilisateur AWS License Manager

API du Gestionnaire de licences

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

1. ListLicenseConfigurations
2. ListAssociationsForLicenseConfiguration
3. ListUsageForLicenseConfiguration

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

Par exemple : supposons que vous utilisiez deux produits sous licence (SQL Service 2017 et Oracle Database Enterprise Edition). Tout d'abord, l'activité `GetLicenseManagerSummary` appelle l'API ListLicenseConfigurations, qui fournit des détails sur les configurations de licence de votre compte. Elle ajoute ensuite des données contextuelles supplémentaires pour chaque configuration de licence en appelant ListUsageForLicenseConfiguration et ListAssociationsForLicenseConfiguration. Enfin, elle convertit les données de configuration de licence en preuves et les associe aux contrôles respectifs du framework (4.5 - Licence gérée par le client pour SQL Server 2017 et 3.0.4 - Licence gérée par le client pour Oracle Database Enterprise Edition). Si vous utilisez un produit sous licence qui n'est couvert par aucun des contrôles du framework, ces données de configuration de licence sont jointes en tant que preuve au contrôle suivant : 5.0 - Licence gérée par le client pour les autres licences.

AWSBonnes pratiques de sécurité de base

AWS Audit Manager fournit un framework standard prédéfini qui prend en charge les bonnes pratiques de sécurité de base AWS.

Rubriques

- Que sont les bonnes pratiques de sécurité de base AWS ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources AWS supplémentaires sur les bonnes pratiques de sécurité de base

Que sont les bonnes pratiques de sécurité de base AWS ?

La norme concernant les bonnes pratiques de sécurité de base AWS est un ensemble de contrôles qui détectent lorsque vos comptes et ressources déployés s'écartent des bonnes pratiques de sécurité.

La norme vous permet d'évaluer en permanence l'ensemble de vos Comptes AWS et charges de travail, afin d'identifier rapidement les écarts par rapport aux bonnes pratiques. La norme fournit des conseils pratiques et prescriptifs sur la façon d'améliorer et de maintenir la sécurité de votre organisation.

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

Utiliser ce framework pour faciliter la préparation de votre audit

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

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

Les détails du framework des bonnes pratiques de sécurité de base AWS sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
AWSBonnes pratiques de sécurité de base	154	0	29	AWS Security Hub

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences des bonnes pratiques de sécurité de base AWS. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources AWS supplémentaires sur les bonnes pratiques de sécurité de base

- Norme des bonnes pratiques de sécurité de base AWS dans le Guide de l'utilisateur AWS Security Hub
- Catégories de contrôle dans le Guide de l'utilisateur AWS Security Hub

Bonnes pratiques de fonctionnement pour AWS

AWS Audit Manager fournit un framework prédéfini des bonnes pratiques de fonctionnement (OBP) AWS pour vous aider dans la préparation de votre audit. Ce framework propose un sous-ensemble de contrôles issus de la norme Bonnes pratiques de sécurité de base AWS. Ces contrôles servent de contrôles de base pour détecter lorsque vos comptes et ressources déployés s'écartent des bonnes pratiques de sécurité.

Rubriques

- Que sont les bonnes pratiques de sécurité de base AWS ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources OBP AWS supplémentaires

Que sont les bonnes pratiques de sécurité de base AWS ?

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

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

Utiliser ce framework pour faciliter la préparation de votre audit

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

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

Les détails du framework des bonnes pratiques de fonctionnement AWS sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
Bonnes pratiques de fonctionnement pour AWS	52	0	20	AWS Security Hub

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences des bonnes pratiques de fonctionnement AWS. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources OBP AWS supplémentaires

- Norme des bonnes pratiques de sécurité de base AWS dans le Guide de l'utilisateur AWS Security Hub
- Catégories de contrôle dans le Guide de l'utilisateur AWS Security Hub

AWS Well-Architected

AWS Audit Manager fournit un cadre prédéfini de framework qui structure et automatise les évaluations pour le framework AWS Well-Architected, sur la base des bonnes pratiques AWS.

Rubriques

- Qu'est-ce que AWS Well-Architected ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources AWS Well-Architected supplémentaires

Qu'est-ce que AWS Well-Architected ?

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

Utiliser ce framework pour faciliter la préparation de votre audit

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

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des preuves pertinentes pour votre audit. Après avoir créé une évaluation,

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

Les détails du framework AWS Well-Architected sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
Framework AWS Well-Architected	16	0	2	AWS Config

> **Tip**
>
> Pour consulter les règles AWS Config utilisées comme mappages de sources de données dans ce framework standard, téléchargez le fichier AuditManager_ConfigDataSourceMappings_AWSWell-ArchitectedFramework.zip.

Les contrôles de ce framework ne sont pas destinés à vérifier si vos systèmes sont conformes. De plus, ils ne peuvent garantir que vous réussirez un audit associé au framework AWS Well-Architected.

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework AWS Well-Architected. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources AWS Well-Architected supplémentaires

- AWS Well-Architected
- Documentation sur le framework AWS Well-Architected

Centre canadien pour la cybersécurité - Profil de contrôle de cloud Medium

AWS Audit Manager fournit un framework standard prédéfini qui structure et automatise les évaluations pour le Centre canadien pour la cybersécurité.

Rubriques

- Qu'est-ce que le Centre canadien pour la cybersécurité ?
- Utiliser ce framework pour faciliter la préparation de votre audit

Qu'est-ce que le Centre canadien pour la cybersécurité ?

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

Le profil de contrôle du cloud Medium du CCCS a remplacé le profil PROTECTED B/Medium Integrity/Medium Availability (PBMM) du gouvernement canadien en mai 2020. Le profil de contrôle de sécurité du cloud Medium du CCCS convient si votre organisation utilise des services de cloud

public pour soutenir ses activités commerciales avec des exigences de confidentialité, d'intégrité et de disponibilité (AIC) medium. Les charges de travail soumises à des exigences AIC Medium signifient que la divulgation, la modification ou la perte d'accès non autorisées aux informations ou aux services utilisés par l'activité commerciale peuvent raisonnablement porter un préjudice grave à une personne ou à une organisation ou un préjudice limité à un groupe de personnes. Voici des exemples de ces niveaux de préjudices :

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

Utiliser ce framework pour faciliter la préparation de votre audit

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

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des preuves pertinentes pour votre audit de Profil de contrôle de cloud Medium CCCS. Dans votre évaluation, vous pouvez spécifier les Comptes AWS et services que vous souhaitez inclure dans le périmètre de votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos ressources AWS. Pour ce faire, il se base sur les contrôles définis dans le framework Profil de contrôle de cloud Medium CCCS. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous

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

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
Centre canadien pour la cybersécurité - Medium	206	396	165	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Key Management Service • AWS License Manager

> **Tip**
>
> Pour consulter les règles AWS Config utilisées comme mappages de sources de données dans ce framework standard, téléchargez le fichier AuditManager_ConfigDataSourceMappings_CanadianCentreforCyberSecurity-Medium.zip.

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est faite selon les exigences du Centre canadien pour la cybersécurité - Framework Medium. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.2.0

AWS Audit Manager fournit deux frameworks prédéfinis qui prennent en charge CIS AWS Foundations Benchmark v1.2.0 :

- Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.2.0, niveau 1
- Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.2.0, niveaux 1 et 2

> **Note**
>
> - Pour plus d'informations sur les frameworks Audit Manager compatibles avec la version v1.3.0, consultez Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.3.0.

- Pour plus d'informations sur les frameworks Audit Manager compatibles avec la version v1.4.0, consultez Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.4.0.

Rubriques

- Qu'est-ce que le CIS ?
- Utiliser ces frameworks pour faciliter la préparation de votre audit
- Plus de ressources CIS

Qu'est-ce que le CIS ?

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

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

Différence entre les benchmarks CIS et les contrôles CIS

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

Exemples

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

  Exemple : CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Assurez-vous que l'authentification multifactorielle est activée pour le compte « utilisateur root »

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

- Les contrôles CIS s'appliquent à l'ensemble de votre organisation. Ils ne sont pas spécifiques à un seul produit d'un fournisseur.

  Exemple : CIS Controls v7.1 - Le sous-contrôle 4.5 utilise l'authentification multifactorielle pour tous les accès administratifs

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

Utiliser ces frameworks pour faciliter la préparation de votre audit

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

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

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.2.0, niveau 1	33	3	4	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub
Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.2.0, niveaux 1 et 2	45	4	4	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Identity and Access Management • AWS Security Hub

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

Vous trouverez ces frameworks sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ces frameworks standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les

services pour vous. Cette sélection est effectuée conformément aux exigences des benchmarks CIS. Si vous devez modifier la liste des services concernés par ces frameworks, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour des instructions sur la façon de personnaliser ces frameworks afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Prérequis pour l'utilisation de ces frameworks

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

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

Règle AWS Config requise	Paramètres requis
ACCESS_KEYS_ROTATED	**`maxAccessKeyAge`** • Nombre maximal de jours sans rotation. • Type : Int • Par défaut : 90 jours • Exigence de conformité : 90 jours maximum
CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED	Ne s'applique pas
CLOUD_TRAIL_ENCRYPTION_ENABLED	Ne s'applique pas
CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED	Ne s'applique pas

Règle AWS Config requise	Paramètres requis
CMK_BACKING_KEY_ROTATION_ENABLED	Ne s'applique pas
IAM_PASSWORD_POLICY	**`MaxPasswordAge`** (facultatif) • Nombre de jours avant l'expiration du mot de passe. • Type : int • Par défaut : 90 • Exigence de conformité : 90 jours maximum
IAM_PASSWORD_POLICY	**`MinimumPasswordLength`** (facultatif) • La longueur minimale du mot de passe. • Type : int • Par défaut : 14 • Exigence de conformité : 14 caractères minimum
IAM_PASSWORD_POLICY	**`PasswordReusePrevention`** (facultatif) • Nombre de mots de passe avant d'autoriser la réutilisation. • Type : int • Par défaut : 24 • Exigence de conformité : un minimum de 24 mots de passe avant réutilisation
IAM_PASSWORD_POLICY	**`RequireLowercaseCharacters`** (facultatif) • Au moins un caractère minuscule est requis dans le mot de passe. • Type : booléen • Valeur par défaut : True • Exigence de conformité : au moins un caractère minuscule est requis

Règle AWS Config requise	Paramètres requis
IAM_PASSWORD_POLICY	**`RequireNumbers`** (facultatif) • Au moins un chiffre est requis dans le mot de passe. • Type : booléen • Valeur par défaut : True • Exigence de conformité : au moins un chiffre est requis
IAM_PASSWORD_POLICY	**`RequireSymbols`** (facultatif) • Au moins un symbole est requis dans le mot de passe. • Type : booléen • Valeur par défaut : True • Exigence de conformité : au moins un caractère symbolique est requis
IAM_PASSWORD_POLICY	**`RequireUppercaseCharacters`** (facultatif) • Au moins un caractère majuscule est requis dans le mot de passe. • Type : booléen • Valeur par défaut : True • Exigence de conformité : au moins un caractère majuscule est requis

Règle AWS Config requise	Paramètres requis
IAM_POLICY_IN_USE	**`policyARN`** • Un ARN de politique IAM à vérifier. • Type : chaîne • Exigence de conformité : crée un rôle IAM pour gérer les incidents avec AWS. **`policyUsageType`** (facultatif) • Spécifie si vous souhaitez que la politique soit attachée à un utilisateur, un groupe ou un rôle. • Type : chaîne • Valeurs valides : `IAM_USER` | `IAM_GROUP` | `IAM_ROLE` | `ANY` • Valeur par défaut : `ANY` • Exigence de conformité : associez la politique de confiance au rôle IAM créé
IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS	Ne s'applique pas
IAM_ROOT_ACCESS_KEY_CHECK	Ne s'applique pas
IAM_USER_NO_POLICIES_CHECK	Ne s'applique pas
IAM_USER_UNUSED_CREDENTIALS_CHECK	**`maxCredentialUsageAge`** • Nombre maximal de jours pendant lesquels les informations d'identification ne peuvent être utilisées. • Type : Int • Par défaut : 90 jours • Exigence de conformité : 90 jours ou plus
INCOMING_SSH_DISABLED	Ne s'applique pas

Règle AWS Config requise	Paramètres requis
MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	Ne s'applique pas
MULTI_REGION_CLOUD_TRAIL_ENABLED	Ne s'applique pas

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

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

Plus de ressources CIS

- CIS AWS Foundations Benchmark v1.2.0
- Articles du blog CIS AWS Foundations Benchmark sur le blog de sécurité AWS

Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.3.0

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

- Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.3.0, niveau 1
- Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.3.0, niveaux 1 et 2

> **Note**
>
> Pour plus d'informations sur CIS AWS Foundations Benchmark v1.2.0 et les frameworks AWS Audit Manager qui prennent en charge cette version du benchmark, consultez Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.2.0.

Rubriques

- Qu'est-ce que le CIS ?
- Utiliser ces frameworks pour faciliter la préparation de votre audit
- Plus de ressources CIS

Qu'est-ce que le CIS ?

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

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

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

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

Différence entre les benchmarks CIS et les contrôles CIS

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

Exemples

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

  Exemple : CIS Amazon Web Services Foundations Benchmark v1.3.0 - 1.5 Assurez-vous que l'authentification multifactorielle est activée pour le compte « utilisateur root »

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

  Exemple : CIS Controls v7.1 - Le sous-contrôle 4.5 utilise l'authentification multifactorielle pour tous les accès administratifs

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

Utiliser ces frameworks pour faciliter la préparation de votre audit

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

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

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.3.0, niveau 1	33	5	6	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS Config • AWS CloudTrail

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
				• AWS Identity and Access Management • AWS Security Hub
Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.3.0, niveaux 1 et 2	49	6	6	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

Tip

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

- AuditManager_ConfigDatasourceMappings_CIS-Benchmark-v1.3.0-Level-1.zip
- AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.3.0,Level1-and-2.zip

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

ne vérifie pas automatiquement les contrôles procéduraux qui nécessitent la collecte manuelle de preuves.

Vous trouverez ces frameworks sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ces frameworks standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences des benchmarks CIS. Si vous devez modifier la liste des services concernés par ces frameworks, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour des instructions sur la façon de personnaliser ces frameworks afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Plus de ressources CIS

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

Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.4.0

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

- Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.4.0, niveau 1
- Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.4.0, niveaux 1 et 2

> **Note**
>
> - Pour plus d'informations sur les frameworks Audit Manager compatibles avec la version v1.2.0, consultez Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.2.0.

- Pour plus d'informations sur les frameworks Audit Manager compatibles avec la version v1.3.0, consultez Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.3.0.

Rubriques

- Qu'est-ce que le benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.4.0 ?
- Utiliser ces frameworks pour faciliter la préparation de votre audit
- Plus de ressources CIS

Qu'est-ce que le benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.4.0 ?

CIS Benchmark for CIS Amazon Web Services Foundations Benchmark, v1.4.0, niveaux 1 et 2, fournit des conseils prescriptifs pour configurer les options de sécurité pour un sous-ensemble de services Amazon Web Services. Il met l'accent sur les paramètres fondamentaux, testables et indépendants de l'architecture. Voici certains des services Amazon Web Services concernés par ce document :

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

Différence entre les benchmarks CIS et les contrôles CIS

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

Exemples

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

  Exemple : CIS Amazon Web Services Foundations Benchmark v1.4.0 - 1.5 Assurez-vous que l'authentification multifactorielle est activée pour le compte « utilisateur root »

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

  Exemple : CIS Controls v7.1 - Le sous-contrôle 4.5 utilise l'authentification multifactorielle pour tous les accès administratifs

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

Utiliser ces frameworks pour faciliter la préparation de votre audit

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

En utilisant les frameworks comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des preuves pertinentes pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos ressources AWS. Cette fonction se base sur les contrôles définis dans le framework CIS. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre

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

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.4.0, niveau 1	32	6	7	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management
Benchmark CIS pour CIS Amazon Web Services Foundations Benchmark, v1.4.0, niveaux 1 et 2	50	8	7	• Amazon Elastic Compute Cloud • Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Pour consulter la liste des règles AWS Config utilisées comme mappages de sources de données pour ces frameworks standard, téléchargez les fichiers suivants :
>
> - AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.4.0-Level-1.zip
> - AuditManager_ConfigDataSourceMappings_CIS-Benchmark-v1.4.0-Level-1-and-2.zip

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

Vous trouverez ces frameworks sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ces frameworks standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences des benchmarks CIS. Si vous devez modifier la liste des services concernés par ces frameworks, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour des instructions sur la façon de personnaliser ces frameworks afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Plus de ressources CIS

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

Groupe 1 de mise en œuvre des Contrôles CIS v7.1

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

> **Note**
>
> Pour plus d'informations sur les contrôles CIS v8 IG1 et le framework AWS Audit Manager qui prend en charge cette norme, consultez Groupe 1 de mise en œuvre des contrôles CIS v8.

AWS Audit Manager fournit un framework prédéfini qui prend en charge Center for Internet Security (CIS) pour vous aider à préparer votre audit.

Rubriques

- Que sont les contrôles CIS ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Plus de ressources CIS

Que sont les contrôles CIS ?

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

Différence entre les benchmarks CIS et les contrôles CIS

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

Exemples

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

  - Exemple : CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Assurez-vous que l'authentification multifactorielle est activée pour le compte « utilisateur root ».
  - Cette recommandation fournit des conseils prescriptifs sur la manière de vérifier cela et de le définir sur le compte racine de l'environnement AWS.
- Les contrôles CIS s'adressent à l'ensemble de votre organisation et ne sont pas spécifiques à un seul produit fournisseur.
  - Exemple : CIS Controls v7.1 - Le sous-contrôle 4.5 utilise l'authentification multifactorielle pour tous les accès administratifs
  - Ce contrôle décrit ce qui est censé être appliqué au sein de votre organisation. Cependant, il ne décrit pas comment vous devez l'appliquer aux systèmes et aux charges de travail que vous exécutez (quel que soit leur emplacement).

Utiliser ce framework pour faciliter la préparation de votre audit

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

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

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

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
Contrôles CIS v7.1 IG1	21	22	16	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management

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

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences des contrôles CIS. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à

l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Plus de ressources CIS

- Contrôles CIS v7.1 IG1

Groupe 1 de mise en œuvre des contrôles CIS v8

AWS Audit Manager fournit un framework prédéfini qui prend en charge le groupe de mise en œuvre 1 des contrôles du Center for Internet Security (CIS) v8.

> **Note**
>
> Pour plus d'informations sur les contrôles CIS v7.1 IG1 et le framework AWS Audit Manager qui prend en charge cette norme, consultez Groupe 1 de mise en œuvre des Contrôles CIS v7.1.

Rubriques

- Que sont les contrôles CIS ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Plus de ressources CIS

Que sont les contrôles CIS ?

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

renforce la sécurité des entreprises lors de leur transition vers des environnements entièrement cloud et hybrides.

Différence entre les benchmarks CIS et les contrôles CIS

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

Exemples

- Les benchmarks CIS sont prescriptifs. Ils font généralement référence à un paramètre spécifique qui peut être revu et défini dans le produit du fournisseur.
  - Exemple : CIS Amazon Web Services Foundations Benchmark v1.2.0 - 1.13 Assurez-vous que l'authentification multifactorielle est activée pour le compte « utilisateur root ».
  - Cette recommandation fournit des conseils prescriptifs sur la manière de vérifier cela et de le définir sur le compte racine de l'environnement AWS.
- Les contrôles CIS s'adressent à l'ensemble de votre organisation et ne sont pas spécifiques à un seul produit fournisseur.
  - Exemple : CIS Controls v7.1 - Le sous-contrôle 4.5 utilise l'authentification multifactorielle pour tous les accès administratifs
  - Ce contrôle décrit ce qui est censé être appliqué au sein de votre organisation. Cependant, il ne décrit pas comment vous devez l'appliquer aux systèmes et aux charges de travail que vous exécutez (quel que soit leur emplacement).

Utiliser ce framework pour faciliter la préparation de votre audit

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

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des preuves pertinentes pour votre audit. Après avoir créé une évaluation,

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

Les détails du framework Contrôles CIS v8 sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
Contrôles CIS v8 IG1	25	31	15	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management • AWS License Manager

> **Tip**
>
> Pour consulter les règles AWS Config utilisées comme mappages de sources de données dans ce framework standard, téléchargez le fichier AuditManager_ConfigDataSourceMappings_CIS-Controls-v8-IG1.zip.

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences des contrôles CIS. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Plus de ressources CIS

- Contrôles CIS v8

Référence modérée FedRAMP

AWS Audit Manager fournit un framework Référence modérée FedRAMP pour vous aider à préparer votre audit.

Rubriques

- Qu'est-ce que FedRAMP ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources supplémentaires FedRAMP

Qu'est-ce que FedRAMP ?

Le Programme fédéral de gestion des risques et des autorisations (FedRAMP) a été créé en 2011. Il fournit une approche rentable et basée sur les risques pour l'adoption et l'utilisation des services cloud par le gouvernement fédéral américain. FedRAMP permet aux agences fédérales d'utiliser les

technologies cloud modernes, en mettant l'accent sur la sécurité et la protection des informations fédérales.

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

Utiliser ce framework pour faciliter la préparation de votre audit

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

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

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

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
Référence modérée FedRAMP	303	908	325	• Amazon Elastic Compute Cloud • AWS Config • AWS Identity and Access Management

> **Tip**
>
> Pour consulter les règles AWS Config utilisées comme mappages de sources de données dans ce framework standard, téléchargez le fichier AuditManager_ConfigDataSourceMappings_FedRAMP-Moderate-Baseline.zip.

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework FedRAMP. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources supplémentaires FedRAMP

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

Règlement général sur la protection des données (RGPD)

AWS Audit Manager fournit un framework standard prédéfini qui soutient le règlement général sur la protection des données (RGPD). Par défaut, ce framework contient uniquement des contrôles manuels. Ces contrôles manuels ne collectent pas automatiquement des preuves. Toutefois, si vous souhaitez automatiser la collecte de preuves pour certains contrôles dans le cadre du RGPD, vous pouvez utiliser la fonction de contrôle personnalisé dans AWS Audit Manager. Pour de plus amples informations, veuillez consulter Utiliser ce framework pour faciliter la préparation de votre audit.

Rubriques

- Qu'est-ce que le Règlement général sur la protection des données (RGPD) ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources supplémentaires sur le RGPD

Qu'est-ce que le Règlement général sur la protection des données (RGPD) ?

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

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

Vous pouvez trouver le framework RGPD sur la page Bibliothèque de frameworks de AWS Audit Manager. Pour plus d'informations, consultez le Centre du règlement général sur la protection des données (RGPD).

Utiliser ce framework pour faciliter la préparation de votre audit

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

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
RGPD	0	371	10	Aucun

Vous trouverez ce framework RGPD sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager. Étant donné que ce framework standard contient uniquement des contrôles manuels, aucun des Services AWS n'est concerné.

> **Note**
>
> Si vous souhaitez automatiser la collecte de preuves pour le RGPD, vous pouvez utiliser Audit Manager pour créer vos propres contrôles personnalisés pour le RGPD. Le tableau suivant fournit des recommandations sur les sources de données AWS que vous pouvez associer aux exigences du RGPD dans vos contrôles personnalisés. Bien que certaines des sources de données suivantes soient associées à plusieurs contrôles, n'oubliez pas que vous n'êtes facturé qu'une seule fois pour chaque évaluation des ressources.
> Les recommandations suivantes utilisent AWS Config et AWS Security Hub comme sources de données. Pour collecter des preuves à partir de ces sources de données, veillez à exécuter les actions suivantes :
>
> - Vérifiez que vous avez suivi les instructions pour activer et configurer AWS Config et AWS Security Hub dans votre Compte AWS.
> - Vérifiez que vous avez inclus les deux AWS Config ainsi que Security Hub en tant que services dans le champ d'application. Pour consulter la liste des services concernés par votre évaluation, rendez-vous sur l'onglet Examiner une évaluation, Services AWS. Pour modifier cette liste, consultez Modifier Services AWS dans le champ d'application.
>
> Une fois que les deux services ont été configurés, Audit Manager collecte des preuves à chaque fois que l'évaluation d'une règle AWS Config spécifique au contrôle Security Hub a lieu.

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

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5) • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10)

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

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

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5) • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10)

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

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

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• 1.10 (IAM.16) • 1.11 (IAM.17) • 1.12 (IAM.4) • 1.13 (IAM.9) • 1.14 (IAM.6) • 1.16 (IAM.2) • 1.2 (IAM.5) • 1.20 (IAM.18) • 1.22 (IAM.1 • 1.3 (IAM.8) • 1.4 (IAM.3) • 1.5 (IAM.11) • 1.6 (IAM.12) • 1.7 (IAM.13) • 1.8 (IAM.14) • 1.9 (IAM.15) • 2.1 (CloudTrail.1) • 2.2 (CloudTrail.4) • 2.3 (CloudTrail.6) • 2.4 (CloudTrail.5) • 2.5 (Config.1) • 2.6 (CloudTrail.7) • 2.7 (CloudTrail.2) • 2.8 (KMS.4) • 2.9 (EC2.6) • 3.1 (CloudWatch.2) • 3.10 (CloudWatch.10)

Nom du contrôle	Ensemble de contrôles	Mappage des sources de données de contrôle recommandé
		• 3.11 (CloudWatch.11) • 3.12 (CloudWatch.12) • 3.13 (CloudWatch.13) • 3.14 (CloudWatch.14) • Config.1

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Après avoir créé vos nouveaux contrôles personnalisés, vous pouvez les ajouter à un framework RGPD personnalisé. Pour plus d'informations, consultez Création d'un framework personnalisé et Modification d'un framework personnalisé. Vous pouvez créer une évaluation à partir de n'importe quel framework RGPD. De cette façon, AWS Audit Manager peut collecter automatiquement des preuves pour les contrôles personnalisés que vous avez ajoutés. Pour des instructions sur la façon de créer une évaluation à l'aide d'un framework, consultez Création d'une évaluation.

Ressources supplémentaires sur le RGPD

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

Loi Gramm-Leach-Bliley

AWS Audit Manager fournit un framework prédéfini qui prend en charge la Loi Gramm-Leach-Bliley (GLBA).

Rubriques

- Qu'est-ce que la Loi Gramm-Leach-Bliley (GLBA) ?
- Utiliser ce framework pour faciliter la préparation de votre audit

Qu'est-ce que la Loi Gramm-Leach-Bliley (GLBA) ?

La Loi Gramm-Leach-Bliley Act (GLB Act ou GLBA), également connue sous le nom de Financial Service Modernization Act de 1999, est une loi fédérale promulguée aux États-Unis pour contrôler la manière dont les institutions financières traitent les informations privées des individus. La Loi se compose de trois sections. La première est la règle de confidentialité financière, qui réglemente la collecte et la divulgation d'informations financières privées. La deuxième est la règle de sauvegarde, qui stipule que les institutions financières doivent mettre en œuvre des programmes de sécurité pour

protéger ces informations. La troisième concerne les dispositions relatives au faux-semblant, qui interdisent la pratique du faux-semblant (accès à des informations privées sous de faux prétextes). La Loi oblige également les institutions financières à fournir à leurs clients des avis de confidentialité écrits expliquant leurs pratiques en matière de partage d'informations.

Utiliser ce framework pour faciliter la préparation de votre audit

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

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

Les détails du framework GLBA sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
Loi Gramm-Leach-Bliley (GLBA)	4	110	16	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
				• AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Pour consulter les règles AWS Config utilisées comme mappages de sources de données dans ce framework standard, téléchargez le fichier AuditManager_ConfigDataSourceMappings_GLBA.zip.

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

Vous trouverez ce framework GLBA sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework GLBA. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

GxP 21 CFR partie 11

AWS Audit Manager fournit un framework prédéfini qui prend en charge les réglementations GxP CFR partie 11 sur la base des bonnes pratiques AWS.

> **Note**
>
> Pour plus d'informations sur l'annexe 11 de la GxP EU et le framework Audit Manager qui la prend en charge, consultez Annexe 11 du GxP EU.

Rubriques

- Qu'est-ce que le GxP CFR partie 11 ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources GxP supplémentaires

Qu'est-ce que le GxP CFR partie 11 ?

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

Le terme GxP englobe un large éventail d'activités liées à la conformité. Il s'agit notamment des bonnes pratiques de laboratoire (GLP), des bonnes pratiques cliniques (GCP) et des bonnes pratiques de fabrication (GMP). Chacun de ces différents types d'activités implique des exigences spécifiques aux produits que les organisations du secteur des sciences de la vie doivent mettre en œuvre. Cela est basé sur le type de produits fabriqués par les organisations ainsi que sur le pays où leurs produits sont vendus. Lorsque les organisations du secteur des sciences de la vie utilisent des systèmes informatisés pour effectuer certaines activités GxP, elles doivent s'assurer que le système GxP informatisé est développé, validé et exploité de manière appropriée pour l'utilisation prévue du système.

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

Utiliser ce framework pour faciliter la préparation de votre audit

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

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

Les détails du framework GxP CFR partie 11 sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
GxP 21 CFR partie 11	13	14	7	• AWS CloudTrail • AWS Config • AWS Identity and Access Management

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

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework GxP CFR partie 11. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources GxP supplémentaires

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

Annexe 11 du GxP EU

AWS Audit Manager fournit un framework prédéfini qui prend en charge les réglementations de l'Annexe 11 du GxP EU sur la base des bonnes pratiques AWS.

> **Note**
>
> Pour plus d'informations sur GxP 21 CFR partie 11 et le framework Audit Manager qui la prend en charge, consultez GxP 21 CFR partie 11.

Rubriques

- Qu'est-ce que l'annexe 11 de la GxP EU ?
- Utiliser ce framework pour faciliter la préparation de votre audit

Qu'est-ce que l'annexe 11 de la GxP EU ?

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

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

Utiliser ce framework pour faciliter la préparation de votre audit

Vous pouvez utiliser le framework GxP EU Annexe 11 pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences GxP. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

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

Les détails du framework GxP EU Annexe 11 sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
Annexe 11 du GxP EU	19	13	3	• Amazon CloudWatch • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Pour consulter les règles AWS Config utilisées comme mappages de sources de données dans ce framework standard, téléchargez le fichier AuditManager_ConfigDataSourceMappings_GxP-EU-Annex-11.zip.

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework GxP EU Annexe 11. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Règle de sécurité Health Insurance Portability and Accountability Act (HIPAA) de 2003

AWS Audit Manager fournit un framework prédéfini qui prend en charge les règles HIPAA pour vous aider dans la préparation de votre audit.

> **Note**
>
> Ce framework était auparavant nommé HIPAA dans la bibliothèque de frameworks. Le 8 mars 2023, ce framework a été rebaptisé HIPAA Security Rule 2003 afin de le différencier de HIPAA Final Omnibus Security Rule 2013.
> Pour plus d'informations sur HIPAA Final Omnibus Security Rule 2013 et le framework Audit Manager qui prend en charge cette norme, consultez Health Insurance Portability and Accountability Act (HIPAA) Final Omnibus Security Rule 2013.

Rubriques

- Qu'est-ce que HIPAA et HIPAA Security Rule 2003 ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources supplémentaires sur HIPAA

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

La loi américaine Health Insurance Portability and Accountability Act (HIPAA) de 1996 aide les travailleurs américains à conserver leur couverture d'assurance maladie lorsqu'ils changent d'emploi ou le perdent. La législation vise également à encourager les dossiers médicaux électroniques afin d'améliorer l'efficacité et la qualité du système de santé américain grâce à un meilleur partage d'informations.

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

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

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

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

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

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

Utiliser ce framework pour faciliter la préparation de votre audit

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

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

Les détails du framework HIPAA Security Rule 2003 sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
HIPAA Security Rule 2003	35	53	5	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

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

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework HIPAA.

Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources supplémentaires sur HIPAA

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

Health Insurance Portability and Accountability Act (HIPAA) Final Omnibus Security Rule 2013

AWS Audit Manager fournit un framework prédéfini qui prend en charge les règles HIPAA pour vous aider dans la préparation de votre audit.

> **Note**
>
> Pour plus d'informations sur HIPAA Security Rule 2003 et le framework AWS Audit Manager qui prend en charge cette norme, consultez Règle de sécurité Health Insurance Portability and Accountability Act (HIPAA) de 2003.

Rubriques

- Qu'est-ce que la loi HIPAA et HIPAA Final Omnibus Security Rule ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources supplémentaires sur HIPAA

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

La loi américaine Health Insurance Portability and Accountability Act (HIPAA) de 1996 aide les travailleurs américains à conserver leur couverture d'assurance maladie lorsqu'ils changent d'emploi ou le perdent. La législation vise également à encourager les dossiers médicaux électroniques afin d'améliorer l'efficacité et la qualité du système de santé américain grâce à un meilleur partage d'informations.

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

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

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

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

De plus en plus de prestataires de soins de santé, de payeurs et de professionnels de l'informatique utilisent des services cloud AWS basés sur des utilitaires pour traiter, stocker et transmettre les informations protégées relatives à la santé (PHI). AWS permet aux entités couvertes et à leurs associés commerciaux soumis à la loi HIPAA d'utiliser l'environnement AWS sécurisé pour traiter, gérer et stocker les informations protégées relatives à la santé. Pour obtenir des instructions sur la manière dont vous pouvez utiliser AWS pour le traitement et le stockage des informations relatives à la santé, consultez le livre blanc Architecture for HIPAA Security and Compliance sur Amazon Web Services.

Utiliser ce framework pour faciliter la préparation de votre audit

Vous pouvez utiliser le framework HIPAA Final Omnibus Security Rule 2013 pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences HIPAA. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

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

Les détails du framework HIPAA Final Omnibus Security Rule 2013 sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
HIPAA Final Omnibus Security Rule 2013	39	46	5	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Pour consulter les règles AWS Config utilisées comme mappages de sources de données dans ce framework standard, téléchargez le fichier AuditManager_ConfigDataSourceMappings_HIPAA-Final-Omnibus-Security-Rule-2013.zip.

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework HIPAA. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources supplémentaires sur HIPAA

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

ISO/IEC 27001:2013 Annexe A

AWS Audit Manager fournit un framework standard prédéfini qui structure et automatise les évaluations conformément à l'annexe A de la norme ISO/CEI 27001:2013.

Rubriques

- Qu'est-ce que l'annexe A de la norme ISO/IEC 27001:2013 ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources supplémentaires sur la norme ISO/IEC 27001:2013 Annexe A

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

La Commission électrotechnique internationale (CEI) et l'Organisation internationale de normalisation (ISO) sont toutes deux des organisations indépendantes, non gouvernementales et à but non lucratif qui élaborent et publient des normes internationales entièrement fondées sur le consensus.

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

Utiliser ce framework pour faciliter la préparation de votre audit

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

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des preuves pertinentes pour votre audit ISO/IEC 27001:2013 Annexe

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

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
ISO/IEC 27001:2013 Annexe A	50	64	35	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Pour consulter les règles AWS Config utilisées comme mappages de sources de données dans ce framework standard, téléchargez le fichier AuditManager_ConfigDataSourceMappings_ISO-IEC-27001-2013-Annex-A.zip.

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

Vous trouverez ce framework ISO/IEC 27001:2013 Annexe A sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework ISO/IEC 27001:2013 Annexe A. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour des instructions sur la façon de créer une évaluation à l'aide de ce framework, consultez Création d'une évaluation. Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources supplémentaires sur la norme ISO/IEC 27001:2013 Annexe A

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

NIST 800-53 (Rev. 5) Low-Moderate-High

AWS Audit Manager fournit un framework prédéfini qui structure et automatise les évaluations pour la norme de conformité NIST 800-53, sur la base des bonnes pratiques AWS.

> **Note**
>
> - Pour plus d'informations sur le framework Audit Manager prenant en charge NIST 800-171, consultez NIST SP 800-171 (Rev. 2).

- Pour plus d'informations sur le framework Audit Manager prenant en charge le framework NIST Cybersecurity, consultez Framework de cybersécurité du NIST version 1.1.

Rubriques

- Qu'est-ce que NIST 800-53 ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources supplémentaires du NIST

Qu'est-ce que NIST 800-53 ?

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

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

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

Utiliser ce framework pour faciliter la préparation de votre audit

Vous pouvez utiliser le framework NIST 800-53 (Rev. 5) Low-Moderate-High pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences du NIST. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des preuves pertinentes pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos ressources AWS. Pour ce faire, il se base sur les contrôles définis dans le framework NIST 800-53 (Rev. 5) Low-Moderate-High. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework NIST 800-53 (Rev. 5) Low-Moderate-High sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
NIST 800-53 (Rev. 5) Low-Moderate-High	225	782	280	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Pour consulter les règles AWS Config utilisées comme mappages de sources de données dans ce framework standard, téléchargez le fichier AuditManager_ConfigDataSourceMappings_NIST-800-53-Rev.5-Low-Moderate-High.zip.

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework NIST 800-53 (Rev. 5) Low-Moderate-High. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources supplémentaires du NIST

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

Framework de cybersécurité du NIST version 1.1

AWS Audit Manager fournit un framework prédéfini qui structure et automatise les évaluations du framework de cybersécurité du NIST, sur la base des bonnes pratiques AWS.

> **Note**
>
> - Pour plus d'informations sur le framework Audit Manager prenant en charge NIST 800-53 (Rev. 5) Low-Moderate-High, consultez NIST 800-53 (Rev. 5) Low-Moderate-High.
> - Pour plus d'informations sur le framework Audit Manager prenant en charge NIST SP 800-171 (Rev. 2), consultez NIST SP 800-171 (Rev. 2).

Rubriques

- Qu'est-ce que le framework de cybersécurité du NIST ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources supplémentaires du NIST

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

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

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

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

Utiliser ce framework pour faciliter la préparation de votre audit

Vous pouvez utiliser le framework de cybersécurité du NIST version 1.1 pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences du NIST CSF. Audit Manager prend actuellement en charge le framework de base en proposant 56 contrôles automatisés et 52 contrôles manuels. Ces contrôles correspondent à 23 catégories de cybersécurité définies dans le framework de base. Audit Manager ne prend pas en charge le profil et les composants de mise en œuvre de ce framework.

Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des preuves pertinentes pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos ressources AWS. Pour ce faire, il se base sur les contrôles définis dans le framework NIST Cybersecurity version 1.1. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails de la version 1.1 du framework de cybersécurité du NIST sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
Framework de cybersécurité du NIST version 1.1	56	52	23	• AWS Config • AWS Identity and Access Management • AWS Security Hub

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

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework de cybersécurité du NIST version 1.1. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources supplémentaires du NIST

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

NIST SP 800-171 (Rev. 2)

AWS Audit Manager fournit un framework prédéfini qui structure et automatise les évaluations pour la norme de conformité NIST SP 800-171 sur la base des bonnes pratiques AWS.

> **Note**
>
> - Pour plus d'informations sur le framework Audit Manager prenant en charge NIST 800-53 (Rev. 5) Low-Moderate-High, consultez NIST 800-53 (Rev. 5) Low-Moderate-High.
> - Pour plus d'informations sur le framework Audit Manager compatible avec le framework de cybersécurité NIST version 1.1, consultez Framework de cybersécurité du NIST version 1.1.

Rubriques

- Qu'est-ce que NIST SP 800-171 ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources supplémentaires du NIST

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

NIST SP 800-171 se concentre sur la protection de la confidentialité des informations non classifiées contrôlées (CUI) dans les systèmes et organisations non fédéraux. Il recommande des exigences

de sécurité spécifiques pour atteindre cet objectif. NIST 800-171 est une publication qui décrit les normes et pratiques de sécurité requises pour les organisations non fédérales qui gèrent des CUI sur leurs réseaux. Elle a été publiée pour la première fois en juin 2015 par le National Institute of Standards and Technology (NIST). Le NIST est une agence gouvernementale américaine qui a publié plusieurs normes et publications pour renforcer la résilience à la cybersécurité dans les secteurs public et privé. Le NIST 800-171 a reçu des mises à jour régulières en fonction des cybermenaces émergentes et de l'évolution des technologies. La dernière version (révision 2) a été publiée en février 2020.

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

Utiliser ce framework pour faciliter la préparation de votre audit

Vous pouvez utiliser le framework NIST SP 800-171 Rev. 2 pour vous aider à vous préparer aux audits. Ce framework comprend un ensemble prédéfini de contrôles avec des descriptions et des procédures de test. Ces contrôles sont regroupés en ensembles de contrôles conformément aux exigences du NIST. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

En utilisant le framework comme point de départ, vous pouvez créer une évaluation Audit Manager et commencer à collecter des preuves pertinentes pour votre audit. Après avoir créé une évaluation, Audit Manager commence à évaluer vos ressources AWS. Pour ce faire, il se base sur les contrôles définis dans le framework NIST SP 800-171 Rev. 2. Au moment d'effectuer un audit, vous (ou le délégué de votre choix) pouvez examiner les preuves collectées par Audit Manager. Vous pouvez parcourir les dossiers de preuves dans votre évaluation et sélectionner les preuves que vous souhaitez inclure dans votre rapport d'évaluation. Ou, si vous avez activé l'outil de recherche de preuves, vous pouvez rechercher des preuves spécifiques et les exporter au format CSV, ou créer un rapport d'évaluation à partir des résultats de votre recherche. Dans tous les cas, vous pouvez utiliser ce rapport d'évaluation pour attester le bon fonctionnement de vos contrôles.

Les détails du framework NIST SP 800-171 Rev. 2 sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
NIST SP 800-171 Rev. 2	66	58	16	• Amazon CloudWatch • Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

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

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

Pour des instructions sur la façon de créer une évaluation avec ce framework, consultez Création d'une évaluation.

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée.

En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework NIST SP 800-171 Rev. 2. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources supplémentaires du NIST

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

PCI DSS V3.2.1

AWS Audit Manager fournit un framework prédéfini qui prend en charge la norme PCI DSS v3.2.1.

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

Rubriques

- Qu'est-ce que la norme PCI DSS ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources PCI DSS supplémentaires

Qu'est-ce que la norme PCI DSS ?

La norme PCI (Payment Card Industry) DSS (Data Security Standard) est une norme sur la sécurité des informations propriétaires. Elle est administrée par le Conseil des normes de sécurité PCI,

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

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

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

Utiliser ce framework pour faciliter la préparation de votre audit

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

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

Les détails du framework PCI DSS V3.2.1 sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
PCI DSS V3.2.1	175	487	12	• Amazon Elastic Compute Cloud • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Pour consulter les règles AWS Config utilisées comme mappages de sources de données dans ce framework standard, téléchargez le fichier AuditManager_ConfigDataSourceMappings_PCI-DSS-V3.2.1.zip.

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

Pour des instructions sur la façon de créer une évaluation avec ce framework, consultez Création d'une évaluation.

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework PCI

DSS V3.2.1. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources PCI DSS supplémentaires

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

PCI DSS V4.0

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

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

Rubriques

- Qu'est-ce que la norme PCI DSS ?
- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources PCI DSS supplémentaires

Qu'est-ce que la norme PCI DSS ?

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

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

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

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

Pour plus d'informations sur les modifications, consultez le Récapitulatif des modifications apportées entre les versions 3.2.1 et 4.0 de la norme PCI DSS.

Utiliser ce framework pour faciliter la préparation de votre audit

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

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

DSS v4.0. Vous pouvez également personnaliser ce framework et ses contrôles pour prendre en charge les audits internes répondant à des exigences spécifiques.

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

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
PCI DSS v4.0	152	128	15	• Amazon API Gateway • Amazon CloudFront • Amazon CloudWatch • Amazon DynamoDB • Amazon Elastic Compute Cloud • Amazon OpenSearch Service • Amazon Redshift • Amazon Relationa

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
				l Database Service • Amazon SageMaker • Amazon Simple Storage Service • AWS Backup • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS KMS • AWS Secrets Manager • AWS Security Hub • AWS WAF

> **Tip**
>
> Pour consulter les règles AWS Config utilisées comme mappages de sources de données dans ce framework standard, téléchargez le fichier AuditManager_ConfigDataSourceMappings_PCI-DSS-V4.zip.

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

Pour des instructions sur la façon de créer une évaluation avec ce framework, consultez Création d'une évaluation.

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework PCI DSS V4. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources PCI DSS supplémentaires

- Centre de ressources relatives à la norme PCI DSS v4.0
- Conseil des normes de sécurité PCI
- Bibliothèque de documents du Conseil des normes de sécurité PCI.
- Page de conformité AWS pour la norme PCI DSS
- Norme de sécurité de l'industrie des cartes de paiement (PCI DSS) v4.0 sur le guide de conformité AWS
- Récapitulatif des modifications apportées entre les versions 3.2.1 et 4.0 de la norme PCI DSS

SOC 2

SOC 2 est une procédure d'audit qui garantit la gestion sécurisée des données d'une entreprise. AWS Audit Manager fournit un framework prédéfini qui prend en charge SOC 2.

Rubriques

- Qu'est-ce que SOC 2 ?

- Utiliser ce framework pour faciliter la préparation de votre audit
- Ressources SOC 2 supplémentaires

Qu'est-ce que SOC 2 ?

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

Les rapports SOC AWS sont des comptes rendus rédigés suite à un audit indépendant réalisé par un tiers qui indiquent comment AWS met en œuvre ses principaux contrôles et objectifs de conformité. Ces rapports sont destinés à vous aider, ainsi que vos auditeurs, à comprendre les mesures de contrôle d'AWS mises en place par en termes d'opérations et de conformité. Il existe cinq rapports SOC AWS :

- Rapport SOC AWS 1, disponible pour les clients AWS auprès d'AWS Artifact.
- Rapport de sécurité, de disponibilité et de confidentialité SOC AWS 2, disponible pour les clients AWS auprès d'AWS Artifact.
- Rapport de sécurité, de disponibilité et de confidentialité SOC AWS 2, disponible pour les clients AWS auprès d'AWS Artifact (n'inclut qu'Amazon DocumentDB).
- Rapport de confidentialité de type I AWS SOC 2, disponible pour les clients AWS auprès d'AWS Artifact.
- Rapport de sécurité, de disponibilité et de confidentialité AWS SOC 3, accessible au public sous forme de livre blanc.

Utiliser ce framework pour faciliter la préparation de votre audit

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

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

Les détails du framework sont les suivants :

Nom du framework dans AWS Audit Manager	Nombre de contrôles automatisés	Nombre de contrôles manuels	Nombre d'ensembles de contrôles	Services AWS dans le champ d'application
SOC 2	20	41	20	• Amazon Elastic Compute Cloud • AWS Auto Scaling • AWS CloudTrail • AWS Config • AWS Identity and Access Management • AWS Security Hub

> **Tip**
>
> Pour consulter les règles AWS Config utilisées comme mappages de sources de données dans ce framework standard, téléchargez le fichier AuditManager_ConfigDataSourceMappings_SOC2.zip.

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

Vous trouverez ce framework sous l'onglet Frameworks standard de Bibliothèque de frameworks dans Audit Manager.

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

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir de ce framework standard, la liste des Services AWS concernés est sélectionnée par défaut et ne peut être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework SOC 2. Si vous devez modifier la liste des services concernés par ce framework, vous pouvez le faire à l'aide des opérations de l'API CreateAssessment ou UpdateAssessment. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Pour obtenir des instructions sur la façon de personnaliser ce framework afin de répondre à vos besoins spécifiques, voir Personnalisation d'un framework existant et Personnalisation d'un contrôle existant.

Ressources SOC 2 supplémentaires

- Page de conformité AWS pour SOC

Bibliothèque de contrôles

Vous pouvez accéder aux contrôles et les gérer à partir de la bibliothèque de contrôles d'Audit Manager. Vous pouvez accéder à la bibliothèque de contrôles à tout moment en choisissant Bibliothèque de contrôles dans le volet de navigation de la console Audit Manager.

La bibliothèque de contrôles contient un catalogue de contrôles standard et de contrôles personnalisés.

- Les contrôles standard sont des contrôles prédéfinis fournis par AWS. Vous pouvez consulter les détails de configuration des contrôles standard, mais vous ne pouvez ni les modifier ni les supprimer. En outre, vous pouvez personnaliser n'importe quel contrôle standard pour en créer un nouveau qui répond à vos besoins spécifiques.
- Les contrôles personnalisés sont des contrôles personnalisés que vous possédez et définissez. Avec un contrôle personnalisé, vous pouvez définir les sources de données à partir desquelles vous souhaitez collecter des éléments probants. Vous pouvez ensuite ajouter des contrôles personnalisés à un framework personnalisé.

  Pour en savoir plus sur la façon d'ajouter un contrôle personnalisé à un framework personnalisé, veuillez consulter la section Bibliothèque de frameworks. Pour en savoir plus sur la création d'une évaluation à partir d'un framework Audit Manager, veuillez consulter la section Évaluations dans AWS Audit Manager.

Cette section décrit comment créer et gérer des contrôles personnalisés dans Audit Manager.

Rubriques

- Accès aux contrôles disponibles dans AWS Audit Manager
- Révision des détails d'un contrôle
- Création d'un contrôle personnalisé
- Modification d'un contrôle personnalisé
- Suppression d'un contrôle personnalisé
- Modification de la fréquence de collecte d'éléments probants pour un contrôle
- Sources de données de contrôle prises en charge pour les éléments probants automatisés

Accès aux contrôles disponibles dans AWS Audit Manager

Vous pouvez consulter tous les contrôles disponibles sur la page Bibliothèque de contrôles de la console Audit Manager. À partir de là, vous pouvez également créer un contrôle personnalisé ou personnaliser un contrôle existant.

Vous pouvez également consulter tous les contrôles disponibles à l'aide de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

Audit Manager console

Pour afficher les contrôles disponibles (console)

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation, choisissez Bibliothèque de contrôles.
3. Choisissez l'onglet Contrôles standard ou l'onglet Contrôles personnalisés pour parcourir les contrôles disponibles.
4. Choisissez le nom du contrôle pour en afficher les détails.

AWS CLI

Pour afficher les contrôles disponibles (AWS CLI)

Exécutez la commande list-controls et spécifiez un `--control-type`. Vous pouvez récupérer la liste des contrôles standards. Vous pouvez également récupérer une liste des contrôles personnalisés.

```
aws auditmanager list-controls --control-type Standard
```

```
aws auditmanager list-controls --control-type Custom
```

Audit Manager API

Pour afficher les contrôles disponibles (API)

Utilisez l'ListControlsopération et spécifiez un ControlType. Vous pouvez renvoyer une liste des contrôles standards. Vous pouvez également renvoyer une liste des contrôles personnalisés.

Pour plus d'informations, choisissez l'un des liens précédents pour en lire davantage dans le Guide de référence de l'APIAWS Audit Manager . Cela inclut des informations sur la façon d'utiliser le `ListControls` fonctionnement et les paramètres dans l'un des SDK spécifiques au langage AWS .

Révision des détails d'un contrôle

Vous pouvez consulter les détails d'un contrôle à l'aide de la console Audit Manager, de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

Audit Manager console

Pour afficher les détails du contrôle (console)

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation, choisissez Bibliothèque de contrôles pour afficher la liste des contrôles disponibles.
3. Choisissez l'onglet Contrôles standard ou l'onglet Contrôles personnalisés pour parcourir les contrôles disponibles.
4. Choisissez le nom du contrôle pour en afficher les détails.

Lorsque vous ouvrez un contrôle, une page de détails s'affiche. Les sections de cette page et leur contenu sont décrits ci-dessous.

Section récapitulative

Cette section fournit une présentation du contrôle. Il contient les informations suivantes :

- Nom du contrôle : le nom du contrôle.
- Type de contrôle : indique s'il s'agit d'un contrôle standard ou personnalisé.
- Balises : le nombre de balises associées au contrôle.
- Types de sources de données : le nombre de types de sources de données utilisés pour ce contrôle.
- Mappages : le nombre d'attributs de mappage utilisés pour récupérer des données à partir d'une source de données.

Si vous consultez un contrôle personnalisé, les informations suivantes sont également affichées :

- Créé par : le compte qui a créé le contrôle personnalisé.
- Date de création : la date à laquelle le contrôle personnalisé a été créé.
- Dernière mise à jour : la date à laquelle le contrôle personnalisé a été modifié pour la dernière fois.

Onglet Détails

Cet onglet fournit un bref aperçu du contrôle. Il contient les informations suivantes :

- La section Description fournit une description du contrôle.
- La section Informations sur les tests fournit une description des procédures de test recommandées pour le contrôle.
- La section Plan d'action décrit les actions recommandées à mettre en œuvre si le contrôle doit être corrigé.

Onglet Sources de données

Cet onglet affiche des informations sur les sources de données du contrôle. Il contient les informations suivantes :

- Nom de la source de données : concerne uniquement les contrôles personnalisés. Il fait référence au nom descriptif que vous avez attribué à chaque source de données. Vous pouvez utiliser ce nom pour faire la distinction entre plusieurs sources de données relevant du même type de source de données.
- Type de source de données : indique d'où proviennent les données probantes.
  - Si Audit Manager collecte les éléments probants, la source de données peut être de quatre types : AWS Security Hub, AWS Config, AWS CloudTrail ou AWS appels d'API.
  - Si vous chargez vos propres éléments probants, le type de source de données est Manuel. Une description indique si l'élément probant manuel requis est un chargement de fichier ou une réponse sous forme de texte.
- Mappage : il s'agit de l'attribut de mappage utilisé pour identifier et récupérer les données de la source de données.
  - Si le type de source de données est AWS Config, le mappage est le nom d'une AWS Config règle spécifique (par exemple,`EC2_INSTANCE_MANAGED_BY_SSM`). Audit Manager utilise ce mappage pour signaler le résultat de cette vérification des règles directement à partir de AWS Config.

- Si le type de source de données est AWS Security Hub, le mappage est le nom d'un contrôle Security Hub spécifique (par exemple,`1.1 – Avoid the use of the "root" account`). Audit Manager utilise ce mappage pour signaler le résultat de ce contrôle de sécurité directement à partir du Security Hub.
- Si le type de source de données est un appel d' AWS API, le mappage est le nom d'un appel d'API spécifique (par exemple,`ec2_DescribeSecurityGroups`). Audit Manager utilise ce mappage pour collecter la réponse de l'API.
- Si la source de données est le cas AWS CloudTrail, le mappage est le nom d'un CloudTrail événement spécifique (par exemple,`CreateAccessKey`). Audit Manager utilise ce mappage pour collecter l'activité utilisateur associée à partir de vos CloudTrail journaux.

- Fréquence : indique à quelle fréquence Audit Manager collecte des éléments probants à partir de la source de données. La fréquence varie en fonction du type de source de données. Pour plus d'informations, choisissez la valeur dans la colonne ou consultez Fréquence de collecte des preuves.

Onglet Balises

Cet onglet liste les balises (ou « tags ») associées au contrôle. Il contient les informations suivantes :

- Clé : la clé de la balise (par exemple, une norme de conformité, une réglementation ou une catégorie).
- Valeur : la valeur de la balise.

AWS CLI

Pour afficher les détails du contrôle (AWS CLI)

1. Pour identifier le contrôle que vous souhaitez examiner, exécutez la commande list-controls et spécifiez un `--control-type`. Vous pouvez récupérer la liste des contrôles standards. Vous pouvez également récupérer une liste des contrôles personnalisés.

   Dans l'exemple suivant, remplacez le *`texte de l'espace réservé`* par `Custom` ou `Standard`.

   ```
   aws auditmanager list-controls --control-type Custom/Standard
   ```

La réponse renvoie une liste de contrôles. Recherchez le contrôle que vous souhaitez examiner et prenez note de l'ID du contrôle et de son Amazon Resource Name (ARN).

2. Pour obtenir les détails du contrôle, exécutez la commande get-control et spécifiez le `--control-id`.

   Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations.

   ```
   aws auditmanager get-control --control-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Les détails du contrôle sont renvoyés au format JSON. Pour comprendre ces données, consultez get-control Output dans la référence des contrôlesAWS CLI .

3. Pour voir les balises d'un contrôle, utilisez la list-tags-for-resourcecommande et spécifiez `--resource-arn` celles du contrôle.

   Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations :

   ```
   aws auditmanager list-tags-for-resource --resource-arn arn:aws:auditmanager:us-east-1:111122223333:control/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
   ```

   Pour plus d'informations sur les balises dans l'Audit Manager, consultez Balisage des ressources AWS Audit Manager.

Audit Manager API

Pour afficher les détails du contrôle (API)

1. Pour identifier le contrôle que vous souhaitez examiner, utilisez l'ListControlsopération et spécifiez un ControlType. Vous pouvez renvoyer une liste des contrôles standards. Vous pouvez également renvoyer une liste des contrôles personnalisés.

   Dans la réponse, recherchez le contrôle que vous souhaitez examiner et prenez note de l'ID du contrôle et de l'Amazon Resource Name (ARN).

2. Pour obtenir les détails du contrôle, utilisez l'GetControlopération. Dans la demande, spécifiez le ControlID obtenu à l'étape 1.

Les détails du contrôle sont renvoyés au format JSON. Pour comprendre ces données, consultez la section Éléments de GetControl réponse dans la référence de l'AWS Audit Manager API.

3. Pour voir les balises du contrôle, utilisez l'ListTagsForResourceopération. Dans la demande, spécifiez le contrôle ResourceArn que vous avez obtenu à l'étape 1.

Pour plus d'informations sur les balises dans l'Audit Manager, consultez Balisage des ressources AWS Audit Manager.

Pour plus d'informations sur ces opérations d'API, cliquez sur l'un des liens précédents dans le Guide de référence de l'APIAWS Audit Manager . Cela inclut des informations sur la façon d'utiliser ces opérations et paramètres dans l'un des SDK spécifiques au langage AWS .

Création d'un contrôle personnalisé

Vous pouvez utiliser des contrôles personnalisés pour collecter des éléments probants à partir de sources de données spécifiques que vous définissez.

Tout comme les contrôles standard, les contrôles personnalisés collectent des éléments probants en permanence lorsqu'ils sont actifs dans vos évaluations. Vous pouvez également ajouter des éléments probants manuels aux contrôles personnalisés que vous créez. Chaque élément probant devient un enregistrement qui vous aide à démontrer la conformité aux exigences de votre contrôle personnalisé.

Pour commencer, voici quelques exemples de la façon dont vous pouvez utiliser des contrôles personnalisés :

Utiliser un contrôle existant comme point de départ

Vous pouvez personnaliser tous les contrôles dans Audit Manager. C'est une bonne option si un contrôle existant répond plus ou moins à votre objectif, mais que vous souhaitez étendre ses indications ou ajuster quelques attributs pour répondre à vos besoins spécifiques. Par exemple, vous pouvez modifier la fréquence à laquelle un contrôle collecte des éléments probants, puis modifier le nom du contrôle en conséquence.

Créer un contrôle personnalisé pour les audits internes

Pour vos audits internes, vous pouvez créer un contrôle personnalisé spécialement conçu qui n'est lié à aucun framework de conformité ou à aucune réglementation spécifique. Cela vous donne la liberté d'adapter les exigences de votre contrôle à un domaine particulier ou de collecter des éléments probants auprès d'une ressource spécifique à l'entreprise. Par exemple, vous pouvez créer un contrôle personnalisé qui utilise les AWS Config règles personnalisées de votre organisation comme source de données pour la collecte de preuves.

Créer une question d'évaluation des risques liés aux fournisseurs

Vous pouvez utiliser des contrôles personnalisés pour faciliter la gestion des évaluations des risques liés aux fournisseurs. Chaque contrôle que vous créez peut représenter une question d'évaluation des risques individuelle. Dans ce cas, le nom du contrôle peut être une question, et vous pouvez fournir une réponse en chargeant un fichier ou en saisissant une réponse sous forme de texte comme élément probant manuel.

Il existe deux façons de créer un contrôle personnalisé. Vous pouvez créer un nouveau contrôle à partir de zéro ou personnaliser un contrôle existant.

Rubriques

- Création d'un nouveau contrôle personnalisé à partir de zéro
- Personnalisation d'un contrôle existant

Création d'un nouveau contrôle personnalisé à partir de zéro

Vous pouvez créer un nouveau contrôle personnalisé à partir de zéro en suivant ces étapes.

> **Important**
>
> Nous vous recommandons vivement de ne jamais placer d'informations identifiables sensibles dans des champs de formulaire tels que Détails de contrôle, Informations de test ou Plan d'action. Si vous créez des contrôles personnalisés contenant des informations sensibles, vous ne pouvez partager aucun de vos frameworks personnalisés contenant ces contrôles.

Rubriques

- Étape 1 : définir les détails du contrôle
- Étape 2 : configurer des sources de données
- Étape 3 (facultatif) : définir un plan d'action
- Étape 4 : vérifier et créer le contrôle
- Que puis-je faire ensuite ?

Étape 1 : définir les détails du contrôle

Commencez par définir les détails de votre contrôle personnalisé.

Pour définir les détails du contrôle

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Bibliothèque de contrôles, puis Création d'un contrôle personnalisé.
3. Sous Détails du contrôle, saisissez les informations suivantes concernant le contrôle.
   - Contrôle : saisissez un nom convivial, un titre ou une question d'évaluation des risques. Cette valeur vous permet d'identifier votre contrôle dans la bibliothèque de contrôles.
   - Description (facultatif) : saisissez les détails pour aider les autres à comprendre l'objectif du contrôle. Cette description apparaît sur la page des détails du contrôle.
4. Sous Informations de test, saisissez les étapes recommandées pour tester le contrôle.
5. Sous Balises, choisissez Ajouter une nouvelle balise pour associer une balise au contrôle. Vous pouvez spécifier une clé pour chaque balise qui décrit le mieux le cadre de conformité pris en charge par ce contrôle. La clé de balise est obligatoire et peut être utilisée comme critère de recherche pour rechercher ce contrôle dans la bibliothèque de contrôles.
6. Choisissez Suivant.

Étape 2 : configurer des sources de données

Définissez ensuite jusqu'à 10 sources de données. Une source de données détermine l'endroit où votre contrôle personnalisé collecte les éléments probants.

Si vous souhaitez collecter des éléments probants automatisés, chaque source de données doit inclure un type de source de données et un mappage de source de données. Ces informations

correspondent à votre AWS utilisation et indiquent à l'Audit Manager où collecter les preuves. Si vous souhaitez plutôt fournir vos propres éléments probants, vous devez nommer votre source de données, puis choisir une option d'élément probant manuel.

> **Important**
>
> Pour utiliser AWS Config correctement Security Hub en tant que sources de données automatisées, veillez à effectuer les opérations suivantes :
>
> - Suivez les instructions pour configurer AWS Config et configurer Security Hub afin de les utiliser avec Audit Manager.
> - Incluez les deux AWS Config , ainsi que Security Hub, parmi les services concernés par votre évaluation.
>
> Audit Manager peut ensuite collecter des preuves chaque fois qu'une évaluation a lieu pour les AWS Config règles ou les contrôles Security Hub que vous spécifiez à cette étape.

Pour configurer des sources de données

1. Sous Nom de la source de données, remplacez le texte de l'espace réservé par un nom descriptif de la source de données.
2. Sous Méthode de collecte d'éléments probants, choisissez la manière dont vous souhaitez collecter les éléments probants pour ce contrôle.

   a. Si vous souhaitez qu'Audit Manager collecte des éléments probants, choisissez Automatisé et procédez comme suit :

      - Sous Type de source de données, spécifiez l'endroit d'où Audit Manager collecte les éléments probants automatisés.
        - Pour AWS CloudTrail, choisissez un mot clé pour le nom de l'événement dans la liste déroulante.
        - Pour AWS Config, sélectionnez un type de règle, puis choisissez un mot-clé d'identification de règles dans la liste déroulante.
        - Pour AWS Security Hub, choisissez un contrôle Security Hub dans la liste déroulante.
        - Pour les appels d'APIAWS , choisissez un appel d'API, puis sélectionnez une fréquence de collecte d'éléments probants.

> **Tip**
>
> Pour un aperçu de chaque type de source de données et des conseils de résolution des problèmes associés, consultez Aperçu des sources de données automatisées.
>
> Si vous devez valider la configuration de votre source de données auprès d'un expert du domaine, définissez pour le moment la méthode de collecte d'éléments probants sur Manuel. Ainsi, vous pouvez créer le contrôle et l'ajouter à un framework dès maintenant, puis le modifier ultérieurement selon vos besoins.

b. Si vous souhaitez fournir vos propres éléments probants, choisissez Manuel, puis sélectionnez une option d'élément probant manuel.

- Chargement de fichier : sélectionnez cette option si le contrôle nécessite une documentation à titre d'élément probant.
- Réponse sous forme de texte : sélectionnez cette option si le contrôle nécessite une réponse à une question d'évaluation des risques.

3. (Facultatif) Sous Détails supplémentaires, saisissez une description de la source de données et une description du dépannage.
4. (Facultatif) Pour ajouter une autre source de données, choisissez Ajouter une source de données, puis répétez les étapes 1 à 3.
5. (Facultatif) Pour supprimer une source de données, choisissez Supprimer en haut de la zone de configuration de la source de données.
6. Lorsque vous avez terminé, choisissez Suivant.

Étape 3 (facultatif) : définir un plan d'action

Indiquez ensuite les actions à entreprendre si ce contrôle doit être corrigé.

Pour définir un plan d'action

1. Sous Titre, saisissez un titre descriptif pour le plan d'action.
2. Sous Instructions du plan d'action, saisissez des instructions détaillées pour le plan d'action.
3. Choisissez Suivant.

Étape 4 : vérifier et créer le contrôle

Vérifiez les informations pour le contrôle Pour modifier les informations d'une étape, choisissez Modifier.

Lorsque vous avez terminé, choisissez Créer un contrôle personnalisé.

Que puis-je faire ensuite ?

Après avoir créé un nouveau contrôle personnalisé, vous pouvez l'ajouter à un framework personnalisé. Pour en savoir plus, veuillez consulter les sections Création d'un framework personnalisé et Modification d'un framework personnalisé.

Après avoir ajouté le contrôle personnalisé à un framework personnalisé, vous pouvez créer une évaluation à partir de ce framework personnalisé et commencer à recueillir des éléments probants. Pour en savoir plus, veuillez consulter la section Création d'une évaluation.

Pour obtenir des conseils de dépannage, veuillez consulter Résolution des problèmes liés aux contrôles et aux ensembles de contrôles.

Personnalisation d'un contrôle existant

Au lieu de créer un tout nouveau contrôle personnalisé, vous pouvez utiliser un contrôle existant comme point de départ et le personnaliser. Dans ce cas, le contrôle existant reste dans la bibliothèque de contrôles et un nouveau contrôle personnalisé est créé avec vos paramètres personnalisés.

Vous pouvez sélectionner n'importe quel contrôle existant à personnaliser. Il peut s'agir d'un contrôle standard ou d'un contrôle personnalisé.

> **Important**
>
> Nous vous recommandons vivement de ne jamais placer d'informations identifiables sensibles dans des champs de formulaire tels que Détails de contrôle, Informations de test ou Plan d'action. Si vous créez des contrôles personnalisés contenant des informations sensibles, vous ne pouvez partager aucun de vos frameworks personnalisés contenant ces contrôles.

Rubriques

- Étape 1 : définir les détails du contrôle
- Étape 2 : configurer des sources de données
- Étape 3 (facultatif) : définir un plan d'action
- Étape 4 : vérifier et créer le contrôle
- Que puis-je faire ensuite ?

Étape 1 : définir les détails du contrôle

Les détails du contrôle sont hérités du contrôle d'origine. Vérifiez et modifiez ces détails si nécessaire.

Pour définir les détails du contrôle

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation, choisissez Bibliothèque de contrôles.
3. Sélectionnez le contrôle que vous souhaitez personnaliser, puis choisissez Personnaliser le contrôle existant.
4. Spécifiez le nouveau nom du contrôle, puis choisissez Personnaliser.
5. Sous Détails du contrôle, personnalisez les détails du contrôle selon vos besoins.
6. Sous Informations de test, personnalisez les informations de test selon vos besoins.
7. Sous Balises, personnalisez les balises selon vos besoins.
8. Choisissez Suivant.

Étape 2 : configurer des sources de données

Les sources de données sont héritées du contrôle d'origine. Vous pouvez modifier, ajouter ou supprimer des sources de données selon vos besoins.

> **Important**
>
> Pour utiliser AWS Config correctement Security Hub en tant que sources de données automatisées, veillez à effectuer les opérations suivantes :
>
> - Suivez les instructions pour configurer AWS Config et configurer Security Hub afin de les utiliser avec Audit Manager.

- Incluez les deux AWS Config , ainsi que Security Hub, parmi les services concernés par votre évaluation.

Audit Manager peut ensuite collecter des preuves chaque fois qu'une évaluation a lieu pour les AWS Config règles ou les contrôles Security Hub que vous spécifiez à cette étape.

Pour configurer des sources de données

1. Sous Nom de la source de données, personnalisez le nom de la source de données selon vos besoins.
2. Sous Méthode de collecte d'éléments probants, personnalisez la sélection selon vos besoins.

   a. Si vous souhaitez qu'Audit Manager collecte des éléments probants, choisissez Automatisé et procédez comme suit :

   - Sous Type de source de données, vérifiez l'endroit à partir duquel Audit Manager collecte les éléments probants automatisés et modifiez-les si nécessaire.
     - Pour AWS CloudTrail, choisissez un mot clé pour le nom de l'événement dans la liste déroulante.
     - Pour AWS Config, sélectionnez un type de règle, puis choisissez un mot-clé d'identification de règles dans la liste déroulante.
     - Pour AWS Security Hub, choisissez un contrôle Security Hub dans la liste déroulante.
     - Pour les appels d'APIAWS , choisissez un appel d'API, puis sélectionnez une fréquence de collecte d'éléments probants.

     > **Tip**
     >
     > Pour un aperçu de chaque type de source de données et des conseils de résolution des problèmes associés, consultez Aperçu des sources de données automatisées.
     > Si vous devez valider la configuration de votre source de données auprès d'un expert du domaine, définissez pour le moment la méthode de collecte d'éléments probants sur Manuel. Ainsi, vous pouvez créer le contrôle et l'ajouter à un framework dès maintenant, puis le modifier ultérieurement selon vos besoins.

b. Si vous souhaitez fournir vos propres éléments probants, choisissez Manuel, puis sélectionnez une option d'élément probant manuel.

   - Chargement de fichier : sélectionnez cette option si le contrôle nécessite une documentation à titre d'élément probant.
   - Réponse sous forme de texte : sélectionnez cette option si le contrôle nécessite une réponse à une question d'évaluation des risques.

3. (Facultatif) Sous Détails supplémentaires, apportez les modifications nécessaires à la description de la source de données ou à la description du dépannage.
4. (Facultatif) Pour ajouter une autre source de données, choisissez Ajouter une source de données.
5. (Facultatif) Pour supprimer une source de données, choisissez Supprimer.
6. Choisissez Suivant.

Étape 3 (facultatif) : définir un plan d'action

Le plan d'action est hérité du contrôle initial. Vous pouvez modifier ce plan d'action selon vos besoins.

Pour définir un plan d'action

1. Sous Titre, vérifiez le titre du plan d'action et personnalisez-le selon vos besoins.
2. Sous Instructions du plan d'action, vérifiez et personnalisez les instructions selon vos besoins.
3. Choisissez Suivant.

Étape 4 : vérifier et créer le contrôle

Vérifiez les informations pour le contrôle Pour modifier les informations d'une étape, choisissez Modifier. Lorsque vous avez terminé, choisissez Créer un contrôle personnalisé.

Que puis-je faire ensuite ?

Après avoir créé un nouveau contrôle personnalisé, vous pouvez l'ajouter à un framework personnalisé. Pour en savoir plus, veuillez consulter les sections Création d'un framework personnalisé et Modification d'un framework personnalisé.

Après avoir ajouté un contrôle personnalisé à un framework personnalisé, vous pouvez créer une évaluation à partir de ce framework personnalisé et commencer à recueillir des éléments probants. Pour en savoir plus, veuillez consulter la section Création d'une évaluation.

Si vous devez modifier un contrôle personnalisé, veuillez consulter Modification d'un contrôle personnalisé.

Pour obtenir des conseils de dépannage, veuillez consulter Résolution des problèmes liés aux contrôles et aux ensembles de contrôles.

Modification d'un contrôle personnalisé

Vous pouvez modifier un contrôle personnalisé dans Audit Manager en suivant les étapes suivantes.

Rubriques

- Étape 1 : modifier les détails du contrôle
- Étape 2 : modifier des sources de données
- Étape 3 : (facultatif) modifier un plan d'action
- Étape 4 : vérifier et mettre à jour le contrôle

Étape 1 : modifier les détails du contrôle

Commencez par vérifier et modifier les détails du contrôle selon vos besoins.

Modifier les détails d'un contrôle

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Bibliothèque de contrôles, puis sélectionnez l'onglet Contrôles personnalisés.
3. Sélectionnez le compte que vous souhaitez modifier puis choisissez Modifier.
4. Sous Détails du contrôle, modifiez les détails du contrôle selon vos besoins.
5. Sous Informations de test, modifiez les informations de test recommandées selon vos besoins.
6. Choisissez Suivant.

> **Tip**
>
> Pour modifier les balises d'un contrôle, ouvrez le contrôle et choisissez l'onglet balises. Vous pouvez y afficher et modifier les balises associées au contrôle.

Étape 2 : modifier des sources de données

Vous pouvez modifier, supprimer ou ajouter des sources de données du contrôle.

> **Important**
>
> Pour utiliser AWS Config correctement Security Hub en tant que sources de données automatisées, veillez à effectuer les opérations suivantes :
>
> - Suivez les instructions pour configurer AWS Config et configurer Security Hub afin de les utiliser avec Audit Manager.
> - Incluez les deux AWS Config , ainsi que Security Hub, parmi les services concernés par votre évaluation.
>
> Audit Manager peut ensuite collecter des preuves chaque fois qu'une évaluation a lieu pour les AWS Config règles ou les contrôles Security Hub que vous spécifiez à cette étape.

Pour modifier des sources de données

1. Sous Nom de la source de données, vérifiez le nom actuel et modifiez-le si nécessaire.
2. Sous Méthode de collecte d'éléments probants, vérifiez la sélection actuelle et modifiez-la si nécessaire.

    a. Si vous souhaitez qu'Audit Manager collecte des éléments probants, choisissez Automatisé et procédez comme suit :

    - Sous Type de source de données, vérifiez l'endroit à partir duquel Audit Manager collecte les éléments probants automatisés et modifiez-les si nécessaire.
        - Pour AWS CloudTrail, choisissez un mot clé pour le nom de l'événement dans la liste déroulante.

- Pour AWS Config, sélectionnez un type de règle, puis choisissez un mot-clé d'identification de règles dans la liste déroulante.
- Pour AWS Security Hub, choisissez un contrôle Security Hub dans la liste déroulante.
- Pour les appels d'APIAWS , choisissez un appel d'API, puis sélectionnez une fréquence de collecte d'éléments probants.

> **Tip**
>
> Pour un aperçu de chaque type de source de données et des conseils de résolution des problèmes associés, consultez Aperçu des sources de données automatisées.

b. Si vous souhaitez fournir vos propres éléments probants, choisissez Manuel, puis sélectionnez une option d'élément probant manuel.

- Chargement de fichier : sélectionnez cette option si le contrôle nécessite une documentation à titre d'élément probant.
- Réponse sous forme de texte : sélectionnez cette option si le contrôle nécessite une réponse à une question d'évaluation des risques.

3. (Facultatif) Sous Détails supplémentaires, apportez les modifications nécessaires à la description de la source de données ou à la description du dépannage.
4. (Facultatif) Pour ajouter une autre source de données, choisissez Ajouter une source de données.
5. (Facultatif) Pour supprimer une source de données, choisissez Supprimer.
6. Choisissez Suivant.

Étape 3 : (facultatif) modifier un plan d'action

Ensuite, passez en revue et modifiez le plan d'action facultatif.

Pour modifier un plan d'action

1. Sous Titre, modifiez le titre selon vos besoins.
2. Sous Instructions du plan d'action, modifiez les instructions selon vos besoins.
3. Choisissez Suivant.

Étape 4 : vérifier et mettre à jour le contrôle

Vérifiez les informations pour le contrôle Pour modifier les informations d'une étape, choisissez Modifier.

Lorsque vous avez terminé, sélectionnez Enregistrer les modifications.

> **Note**
>
> Une fois que vous avez modifié un contrôle, les modifications prennent effet comme suit dans toutes les évaluations actives qui comprennent le contrôle :
>
> - Pour les contrôles utilisant des appels d'APIAWS comme type de source de données, les modifications prennent effet à 00 h 00 UTC le jour suivant.
> - Pour tous les autres contrôles, les modifications prennent effet immédiatement.

Suppression d'un contrôle personnalisé

Vous pouvez utiliser la bibliothèque de contrôles pour supprimer un contrôle personnalisé indésirable. Une fois que vous avez supprimé un contrôle, il n'apparaît plus dans la bibliothèque de contrôles. Vous pouvez également supprimer des contrôles personnalisés à l'aide de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI).

> **Important**
>
> Lorsque vous supprimez un contrôle personnalisé, cette action le supprime de tous les frameworks (ou évaluations) personnalisés auxquels il est actuellement associé. Par conséquent, Audit Manager cesse de collecter des éléments probants pour ce contrôle personnalisé dans toutes vos évaluations. Cela comprend les évaluations que vous avez créées avant de supprimer le contrôle personnalisé.

Audit Manager console

Pour supprimer un contrôle personnalisé (console)

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.

2. Dans le volet de navigation, choisissez Bibliothèque de contrôles, puis sélectionnez l'onglet Contrôles personnalisés.
3. Sélectionnez le compte que vous souhaitez supprimer, puis choisissez Supprimer.
4. Dans la fenêtre contextuelle qui apparaît, choisissez Supprimer pour confirmer la suppression.

AWS CLI

Pour supprimer un contrôle personnalisé (AWS CLI)

1. Tout d'abord, identifiez le contrôle personnalisé que vous souhaitez supprimer. Pour ce faire, exécutez la commande list-controls et spécifiez le `--control-type` en tant que `Custom`.

   ```
   aws auditmanager list-controls --control-type Custom
   ```

   La réponse renvoie une liste de contrôles personnalisés. Recherchez le contrôle que vous souhaitez supprimer et notez son ID.
2. Exécutez ensuite la commande delete-control et utilisez le paramètre `--control-id` pour indiquer le contrôle que vous souhaitez supprimer.

   Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations.

   ```
   aws auditmanager delete-control --control-id a1b2c3d4-5678-90ab-cdef-
   EXAMPLE11111
   ```

Audit Manager API

Pour supprimer un contrôle personnalisé (API)

1. Utilisez l'ListControlsopération et spécifiez le ControlType commeCustom. Dans la réponse, recherchez le contrôle que vous souhaitez supprimer et notez son ID.
2. Utilisez cette DeleteControlopération pour supprimer le contrôle personnalisé. Dans la demande, utilisez le paramètre ControlID pour indiquer le contrôle que vous souhaitez supprimer.

Pour plus d'informations sur ces opérations d'API, cliquez sur l'un des liens précédents dans le Guide de référence de l'APIAWS Audit Manager . Cela inclut des informations sur la façon d'utiliser ces opérations et paramètres dans l'un des SDK spécifiques au langage AWS .

Modification de la fréquence de collecte d'éléments probants pour un contrôle

AWS Audit Manager recueille des preuves provenant de plusieurs sources de données à des fréquences variables. La fréquence de collecte des éléments probants étayés dépend du type d'éléments probants collectés pour le contrôle.

- Pour les appels d'APIAWS , Audit Manager collecte des éléments probants à l'aide d'un appel d'API de description à un autre Service AWS. Vous pouvez définir la fréquence de collecte des éléments probants directement dans Audit Manager (pour les contrôles personnalisés uniquement).
- En effet AWS Config, Audit Manager rapporte le résultat d'un contrôle de conformité directement depuis AWS Config. La fréquence suit les déclencheurs définis dans la règle AWS Config .
- Pour AWS Security Hub, Audit Manager rapporte le résultat d'un contrôle de conformité directement depuis Security Hub. La fréquence suit le calendrier de la vérification de Security Hub.
- Car AWS CloudTrail, Audit Manager collecte des preuves en permanence auprès de CloudTrail. Vous ne pouvez pas modifier la fréquence pour ce type d'élément probant.

Les sections suivantes fournissent plus d'informations sur la fréquence de collecte d'éléments probants pour chaque type de source de données de contrôle et sur la manière de la modifier (le cas échéant).

Rubriques

- Instantanés de configuration issus d'appels d' AWS API
- Contrôles de conformité effectués par AWS Config
- Contrôles de conformité effectués par Security Hub
- Journaux d'activité des utilisateurs provenant de AWS CloudTrail

Instantanés de configuration issus d'appels d' AWS API

> **Note**
>
> Ce qui suit s'applique uniquement aux contrôles personnalisés. Vous ne pouvez pas modifier la fréquence de collecte d'éléments probants pour un contrôle standard qui utilise des appels d'API comme source de données.

Si un contrôle personnalisé utilise des appels d' AWS API comme type de source de données, vous pouvez modifier la fréquence de collecte des preuves dans Audit Manager en suivant ces étapes.

Pour modifier la fréquence de collecte des éléments probants pour un contrôle personnalisé avec une source de données d'appel d'API

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le volet de navigation, choisissez Bibliothèque de contrôles, puis sélectionnez l'onglet Contrôles personnalisés.
3. Choisissez le contrôle personnalisé que vous souhaitez modifier, puis choisissez Modifier.
4. Sur la page Modifier les détails du contrôle, choisissez Modifier.
5. Recherchez la zone de source de données que vous souhaitez modifier et vérifiez que les informations suivantes sont correctes :
   - La méthode de collecte d'éléments probants est définie sur Automatisée.
   - Le type de source de données est celui des appels d'APIAWS .
   - L'appel d'API sélectionné est celui dont vous souhaitez modifier la fréquence.
6. Sous Fréquence, choisissez la fréquence à laquelle vous souhaitez collecter des éléments probants pour le contrôle personnalisé.
7. Répétez les étapes 5 et 6 selon les besoins pour toutes les sources de données d'appels d'API supplémentaires que vous souhaitez modifier.
8. Choisissez Suivant.
9. Sur la page Modifier un plan d'action, choisissez Suivant.
10. Sur la page Vérifier et mettre à jour le contrôle, vérifiez les informations relatives au contrôle personnalisé. Pour modifier les informations d'une étape, choisissez Modifier.

11. Lorsque vous avez terminé, sélectionnez Enregistrer les modifications.

Une fois que vous avez modifié un contrôle avec des appels d'APIAWS comme type de source de données, les modifications prennent effet à 00 h 00 UTC le jour suivant dans toutes les évaluations actives qui comprennent le contrôle.

Contrôles de conformité effectués par AWS Config

> **Note**
>
> Ce qui suit s'applique aux contrôles standard et aux contrôles personnalisés qui utilisent AWS Config Rules comme source de données.

Si un contrôle est utilisé AWS Config comme type de source de données, vous ne pouvez pas modifier la fréquence de collecte des preuves directement dans Audit Manager. Cela est dû au fait que la fréquence suit les déclencheurs définis dans la AWS Config règle.

Il existe deux types de déclencheurs pour AWS Config Rules :

1. Modifications de configuration : AWS Config exécute des évaluations de la règle lorsque certains types de ressources sont créés, modifiés ou supprimés.
2. Périodique : AWS Config exécute des évaluations de la règle à la fréquence que vous choisissez (par exemple, toutes les 24 heures).

Pour en savoir plus sur les déclencheurs pour AWS Config Rules, consultez la section Types de déclencheurs dans le Guide duAWS Config développeur.

Pour obtenir des instructions sur la façon de gérer AWS Config Rules, consultez la section Gestion de vos AWS Config règles.

Contrôles de conformité effectués par Security Hub

> **Note**
>
> Ce qui suit s'applique aux contrôles standard et aux contrôles personnalisés qui utilisent les contrôles de Security Hub comme source de données.

Si un contrôle utilise Security Hub comme type de source de données, vous ne pouvez pas modifier la fréquence de collecte des éléments probants directement dans Audit Manager. En effet, la fréquence suit le calendrier des vérifications de Security Hub.

- Les contrôles périodiques s'exécutent automatiquement dans les 12 heures suivant la dernière exécution. Vous ne pouvez pas modifier la périodicité.
- Les vérifications déclenchées par une modification s'exécutent lorsque l'état de la ressource associée change. Même si la ressource ne change pas d'état, l'heure de mise à jour des vérifications déclenchées par une modification est actualisée toutes les 18 heures. Cela permet d'indiquer que le contrôle est toujours activé. En général, utilise des règles déclenchées par des modifications chaque fois que c'est possible.

Pour en savoir plus, consultez la section Planification de l'exécution des contrôles de sécurité dans le guide de l'utilisateurAWS Security Hub .

Journaux d'activité des utilisateurs provenant de AWS CloudTrail

> **Note**
>
> Ce qui suit s'applique aux contrôles standard et aux contrôles personnalisés qui utilisent les journaux d'activité des utilisateurs AWS CloudTrail comme source de données.

Vous ne pouvez pas modifier la fréquence de collecte des preuves pour les contrôles qui utilisent les journaux d'activité CloudTrail comme type de source de données. L'Audit Manager collecte ce type de CloudTrail preuves de manière continue. La fréquence est continue car l'activité des utilisateurs peut se produire à tout moment de la journée.

Sources de données de contrôle prises en charge pour les éléments probants automatisés

Lorsque vous créez un contrôle personnalisé dans AWS Audit Manager, vous pouvez configurer votre contrôle pour collecter des preuves automatisées à partir des types de sources de données suivants :

- AWS CloudTrail
- AWS Security Hub

- AWS Config
- AWS Appels d'API

Les rubriques suivantes résument chacun de ces types de sources de données automatisées et répertorient les AWS Security Hub contrôles, AWS Config règles et appels d' AWS API spécifiques pris en charge par Audit Manager.

Rubriques

- Aperçu des sources de données automatisées
- AWS Config Rules soutenu par AWS Audit Manager
- AWS Security Hub commandes prises en charge par AWS Audit Manager
- Appels d'API pris en charge par AWS Audit Manager
- AWS CloudTrail noms d'événements pris en charge par AWS Audit Manager

Aperçu des sources de données automatisées

Le tableau suivant fournit un aperçu de chaque type de source de données automatisée.

Type de source de donnée	Descripti on	Fréquence de collecte des éléments probants	Pour utiliser ce type de source de données...	Lorsque ce contrôle est actif dans une évaluation...	Conseils de dépannage associés
AWS CloudTrail	Suit l'activité d'un utilisateur spécifique.	Continu.	Sélectionnez dans la liste des noms d'événements pris en charge.	Audit Manager filtre vos CloudTrail journaux en fonction du mot clé que vous avez choisi. Les résultats sont importés en tant qu'éléments probants de l'activité de l'utilisateur.	Mon évaluation ne collecte pas de preuves de l'activité des utilisate

Type de source de donnée	Description	Fréquence de collecte des éléments probants	Pour utiliser ce type de source de données...	Lorsque ce contrôle est actif dans une évaluation...	Conseils de dépannage associés
					urs auprès d'AWS CloudTrail
AWS Config	Capture un aperçu de la situation en matière de sécurité de vos ressources en rapportant les résultats de AWS Config.	Sur la base des déclencheurs définis dans la AWS Config règle.	Sélectionnez un type de règle, puis sélectionnez une règle. • Sélectionnez les règles gérées dans la liste des mots clés de règles gérées pris en charge. • Sélectionnez les règles personnalisées dans la liste des règles disponibles.	Audit Manager obtient les résultats de cette règle directement auprès de AWS Config. Le résultat est importé en tant qu'élément probant de contrôle de conformité.	Mon évaluation ne collecte pas de preuves pour la vérification de la conformité auprès d'AWS Config AWS Config problèmes d'intégration

Type de source de donnée	Descripti on	Fréquence de collecte des éléments probants	Pour utiliser ce type de source de données...	Lorsque ce contrôle est actif dans une évaluation...	Conseils de dépannage associés
AWS Security Hub	Capture un instantan é du niveau de sécurité de vos ressource s en rapportan t les résultats de Security Hu	Selon le calendrie r de la vérification de Security Hub.	Sélectionnez dans la liste des identifiants de contrôle Security Hub pris en charge.	Audit Manager obtient le résultat du contrôle de sécurité directement depuis Security Hub. Le résultat est importé en tant qu'élément probant de contrôle de conformité.	Mon évaluatio n ne collecte pas de preuves pour la vérificat ion de la conformit é auprès d'AWS Security Hub

Type de source de donnée	Description	Fréquence de collecte des éléments probants	Pour utiliser ce type de source de données...	Lorsque ce contrôle est actif dans une évaluation...	Conseils de dépannage associés
AWS Appels d'API	Prend un instantané de la configuration de vos ressources directement via un appel d'API à l'adresse spécifiée Service AWS.	Quotidien, hebdomadaire ou mensuel.	Sélectionnez dans la liste des appels d'API pris en charge, puis choisissez votre fréquence préférée.	Audit Manager effectue l'appel d'API en fonction de la fréquence que vous spécifiez. La réponse est importée en tant qu'élément probant des données de configuration.	Mon évaluation ne collecte pas de preuves de données de configuration pour un appel d'API AWS

AWS Config Rules soutenu par AWS Audit Manager

Vous pouvez utiliser Audit Manager pour saisir les AWS Config évaluations comme preuves pour les audits. Lorsque vous créez ou modifiez un contrôle personnalisé, vous pouvez spécifier une ou plusieurs AWS Config règles en tant que mappage des sources de données pour la collecte de preuves. AWS Config effectue des contrôles de conformité sur la base de ces règles, et Audit Manager rapporte les résultats à titre de preuve du contrôle de conformité.

Outre les règles gérées, vous pouvez également mapper vos règles personnalisées à une source de données de contrôle.

Note

- Audit Manager ne collecte pas d'éléments probants à partir des règles AWS Config liées aux services, à l'exception des règles liées aux services issues des packs de conformité et de AWS Organizations. Pour plus d'informations, consultez dans la section de résolution des problèmes.
- Audit Manager ne gère pas les AWS Config règles à votre place. Avant de commencer la collecte de preuves, nous vous recommandons de revoir les paramètres de vos AWS Config règles actuelles. Ensuite, validez ces paramètres par rapport aux exigences du framework que vous avez choisi. Si nécessaire, vous pouvez mettre à jour les paramètres d'une règle AWS Config afin qu'elle soit conforme aux exigences du framework. Vous pouvez ainsi garantir que vos évaluations collectent les éléments probants de contrôle de conformité corrects pour ce framework.

  Supposons, par exemple, que vous créez une évaluation pour CIS v1.2.0. Ce framework possède un contrôle nommé 1.9 : assurez-vous que la politique de mot de passe IAM nécessite une longueur minimale de 14 ou plus. Dans AWS Config, la iam-password-policyrègle comporte un `MinimumPasswordLength` paramètre qui vérifie la longueur du mot de passe. La valeur par défaut de ce paramètre est de 14 caractères. Par conséquent, la règle s'aligne sur les exigences de contrôle. Si vous n'utilisez pas la valeur de paramètre par défaut, assurez-vous que la valeur que vous utilisez est égale ou supérieure aux 14 caractères requis par CIS v1.2.0. Vous trouverez les détails des paramètres par défaut pour chaque règle gérée dans la documentationAWS Config.

Rubriques

- Utilisation de règles AWS Config gérées avec Audit Manager
- Utilisation de règles AWS Config personnalisées avec Audit Manager
- Résolution des problèmes liés à AWS Config l'intégration avec Audit Manager

Utilisation de règles AWS Config gérées avec Audit Manager

326 règles AWS Config gérées sont actuellement prises en charge par Audit Manager. Vous pouvez utiliser l'un des mots clés suivants d'identification de règles gérées lorsque vous configurez une source de données pour un contrôle personnalisé. Pour plus d'informations sur les règles

gérées répertoriées ci-dessous, choisissez un élément dans la liste ou consultez la section Règles géréesAWS Config dans le guide de l'utilisateurAWS Config .

> **Tip**
>
> Quand vous choisissez une règle gérée dans la console Audit Manager lors de la création d'un contrôle personnalisé, assurez-vous de rechercher l'un des mots clés suivants d'identification de règle, et non le nom de la règle. Pour plus d'informations sur la différence entre le nom de la règle et l'identifiant de la règle, et sur la manière de trouver l'identifiant d'une règle gérée, consultez la section Dépannage de ce guide de l'utilisateur.

Mots clés de règles AWS Config gérées pris en charge

- ACCESS_KEYS_ROTATED
- ACCOUNT_PART_OF_ORGANIZATIONS
- ACM_CERTIFICATE_EXPIRATION_CHECK
- ACM_CERTIFICATE_RSA_CHECK
- ALB_DESYNC_MODE_CHECK
- ALB_HTTP_DROP_INVALID_HEADER_ENABLED
- ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK
- ALB_WAF_ENABLED
- API_GW_ASSOCIATED_WITH_WAF
- API_GW_CACHE_ENABLED_AND_ENCRYPTED
- API_GW_ENDPOINT_TYPE_CHECK
- API_GW_EXECUTION_LOGGING_ENABLED
- API_GW_SSL_ENABLED
- API_GW_XRAY_ENABLED
- API_GWV2_ACCESS_LOGS_ENABLED
- API_GWV2_AUTHORIZATION_TYPE_CONFIGURED
- APPROVED_AMIS_BY_ID
- APPROVED_AMIS_BY_TAG
- APPSYNC_ASSOCIATED_WITH_WAF

Mots clés de règles AWS Config gérées pris en charge

- APPSYNC_CACHE_ENCRYPTION_AT_REST
- APPSYNC_LOGGING_ENABLED
- AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED
- AURORA_MYSQL_BACKTRACKING_ENABLED
- AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- AUTOSCALING_CAPACITY_REBALANCING
- AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED
- AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT
- AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED
- AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2
- AUTOSCALING_LAUNCH_TEMPLATE
- AUTOSCALING_MULTIPLE_AZ
- AUTOSCALING_MULTIPLE_INSTANCE_TYPES
- BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
- BACKUP_RECOVERY_POINT_ENCRYPTED
- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED
- CLB_DESYNC_MODE_CHECK
- CLB_MULTIPLE_AZ
- CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED
- CLOUD_TRAIL_ENABLED
- CLOUD_TRAIL_ENCRYPTION_ENABLED
- CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED
- CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK
- CLOUDFORMATION_STACK_NOTIFICATION_CHECK
- CLOUDFRONT_ACCESSLOGS_ENABLED
- CLOUDFRONT_ASSOCIATED_WITH_WAF
- CLOUDFRONT_CUSTOM_SSL_CERTIFICATE

Mots clés de règles AWS Config gérées pris en charge

- CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED
- CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS
- CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED
- CLOUDFRONT_ORIGIN_FAILOVER_ENABLED
- CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED
- CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET
- CLOUDFRONT_SECURITY_POLICY_CHECK
- CLOUDFRONT_SNI_ENABLED
- CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED
- CLOUDFRONT_VIEWER_POLICY_HTTPS
- CLOUDTRAIL_S3_DATAEVENTS_ENABLED
- CLOUDTRAIL_SECURITY_TRAIL_ENABLED
- CLOUDWATCH_ALARM_ACTION_CHECK
- CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK
- CLOUDWATCH_ALARM_RESOURCE_CHECK
- CLOUDWATCH_ALARM_SETTINGS_CHECK
- CLOUDWATCH_LOG_GROUP_ENCRYPTED
- CMK_BACKING_KEY_ROTATION_ENABLED
- CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION
- CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK
- CODEBUILD_PROJECT_ENVVAR_ AWSCRED_CHECK
- CODEBUILD_PROJECT_LOGGING_ENABLED
- CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED
- CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK
- CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED
- CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED
- CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED
- CODEPIPELINE_DEPLOYMENT_COUNT_CHECK
- CODEPIPELINE_REGION_FANOUT_CHECK

Mots clés de règles AWS Config gérées pris en charge

- CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED
- CW_LOGGROUP_RETENTION_PERIOD_CHECK
- DAX_ENCRYPTION_ENABLED
- DB_INSTANCE_BACKUP_ENABLED
- DESIRED_INSTANCE_TENANCY
- DESIRED_INSTANCE_TYPE
- DMS_REPLICATION_NOT_PUBLIC
- DYNAMODB_AUTOSCALING_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_PITR_ENABLED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- DYNAMODB_TABLE_ENCRYPTED_KMS
- DYNAMODB_TABLE_ENCRYPTION_ENABLED
- DYNAMODB_THROUGHPUT_LIMIT_CHECK
- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_OPTIMIZED_INSTANCE
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK
- EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL
- EC2_EBS_ENCRYPTION_BY_DEFAULT
- EC2_IMDSV2_CHECK
- EC2_INSTANCE_DETAILED_MONITORING_ENABLED
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_INSTANCE_MULTIPLE_ENI_CHECK
- EC2_INSTANCE_NO_PUBLIC_IP
- EC2_INSTANCE_PROFILE_ATTACHED
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED

Mots clés de règles AWS Config gérées pris en charge

- EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED
- EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED
- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED
- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_MANAGEDINSTANCE_PLATFORM_CHECK
- EC2_NO_AMAZON_KEY_PAIR
- EC2_PARAVIRTUAL_INSTANCE_CHECK
- EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI
- EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC
- EC2_STOPPED_INSTANCE
- EC2_TOKEN_HOP_LIMIT_CHECK
- EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED
- EC2_VOLUME_INUSE_CHECK
- ECR_PRIVATE_IMAGE_SCANNING_ENABLED
- ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED
- ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED
- ECS_ _ACTIVÉ AWSVPC_NETWORKING
- ECS_CONTAINER_INSIGHTS_ENABLED
- ECS_CONTAINERS_NONPRIVILEGED
- ECS_CONTAINERS_READONLY_ACCESS
- ECS_FARGATE_LATEST_PLATFORM_VERSION
- ECS_NO_ENVIRONMENT_SECRETS
- ECS_TASK_DEFINITION_LOG_CONFIGURATION
- ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT
- ECS_TASK_DEFINITION_NONROOT_USER
- ECS_TASK_DEFINITION_PID_MODE_CHECK

Mots clés de règles AWS Config gérées pris en charge

- ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK
- EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY
- EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY
- EFS_ENCRYPTED_CHECK
- EFS_IN_BACKUP_PLAN
- EFS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EIP_ATTACHED
- EKS_CLUSTER_LOGGING_ENABLED
- EKS_CLUSTER_OLDEST_SUPPORTED_VERSION
- EKS_CLUSTER_SUPPORTED_VERSION
- EKS_ENDPOINT_NO_PUBLIC_ACCESS
- EKS_SECRETS_ENCRYPTED
- ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH
- ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED
- ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK
- ELASTICACHE_RBAC_AUTH_ENABLED
- ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK
- ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED
- ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST
- ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT
- ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED
- ELASTICACHE_SUBNET_GROUP_CHECK
- ELASTICACHE_SUPPORTED_ENGINE_VERSION
- ELASTICSEARCH_ENCRYPTED_AT_REST
- ELASTICSEARCH_IN_VPC_ONLY
- ELASTICSEARCH_LOGS_TO_CLOUDWATCH
- ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- ELB_ACM_CERTIFICATE_REQUIRED

Mots clés de règles AWS Config gérées pris en charge

- ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED
- ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK
- ELB_DELETION_PROTECTION_ENABLED
- ELB_LOGGING_ENABLED
- ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK
- ELB_TLS_HTTPS_LISTENERS_ONLY
- ELBV2_ACM_CERTIFICATE_REQUIRED
- ELBV2_MULTIPLE_AZ
- EMR_KERBEROS_ENABLED
- EMR_MASTER_NO_PUBLIC_IP
- ENCRYPTED_VOLUMES
- FMS_SHIELD_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RESOURCE_POLICY_CHECK
- FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK
- FSX_LAST_BACKUP_RECOVERY_POINT_CREATED
- FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- GUARDDUTY_ENABLED_CENTRALIZED
- GUARDDUTY_NON_ARCHIVED_FINDINGS
- IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS
- IAM_GROUP_HAS_USERS_CHECK
- IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS
- IAM_NO_INLINE_POLICY_CHECK
- IAM_PASSWORD_POLICY
- IAM_POLICY_BLACKLISTED_CHECK
- IAM_POLICY_IN_USE
- IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS
- IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS
- IAM_ROLE_MANAGED_POLICY_CHECK
- IAM_ROOT_ACCESS_KEY_CHECK

Mots clés de règles AWS Config gérées pris en charge

- IAM_USER_GROUP_MEMBERSHIP_CHECK
- IAM_USER_MFA_ENABLED
- IAM_USER_NO_POLICIES_CHECK
- IAM_USER_UNUSED_CREDENTIALS_CHECK
- INCOMING_SSH_DISABLED
- INSTANCES_IN_VPC
- KINESIS_STREAM_ENCRYPTED
- INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY
- KMS_CMK_NOT_SCHEDULED_FOR_DELETION
- LAMBDA_CONCURRENCY_CHECK
- LAMBDA_DLQ_CHECK
- LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED
- LAMBDA_FUNCTION_SETTINGS_CHECK
- LAMBDA_INSIDE_VPC
- LAMBDA_VPC_MULTI_AZ_CHECK
- MACIE_STATUS_CHECK
- MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS
- MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED
- MQ_NO_PUBLIC_ACCESS
- MULTI_REGION_CLOUD_TRAIL_ENABLED
- NACL_NO_UNRESTRICTED_SSH_RDP
- NETFW_LOGGING_ENABLED
- NETFW_MULTI_AZ_ENABLED
- NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS
- NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS
- NETFW_POLICY_RULE_GROUP_ASSOCIATED
- NETFW_STATELESS_RULE_GROUP_NOT_EMPTY
- NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED

Mots clés de règles AWS Config gérées pris en charge

- NO_UNRESTRICTED_ROUTE_TO_IGW
- OPENSEARCH_ACCESS_CONTROL_ENABLED
- OPENSEARCH_AUDIT_LOGGING_ENABLED
- OPENSEARCH_DATA_NODE_FAULT_TOLERANCE
- OPENSEARCH_ENCRYPTED_AT_REST
- OPENSEARCH_HTTPS_REQUIRED
- OPENSEARCH_IN_VPC_ONLY
- OPENSEARCH_LOGS_TO_CLOUDWATCH
- OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK
- RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED
- RDS_CLUSTER_DEFAULT_ADMIN_CHECK
- RDS_CLUSTER_DELETION_PROTECTION_ENABLED
- RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED
- RDS_CLUSTER_MULTI_AZ_ENABLED
- RDS_DB_SECURITY_GROUP_NOT_ALLOWED
- RDS_ENHANCED_MONITORING_ENABLED
- RDS_IN_BACKUP_PLAN
- RDS_INSTANCE_DEFAULT_ADMIN_CHECK
- RDS_INSTANCE_DELETION_PROTECTION_ENABLED
- RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED
- RDS_INSTANCE_PUBLIC_ACCESS_CHECK
- RDS_LAST_BACKUP_RECOVERY_POINT_CREATED
- RDS_LOGGING_ENABLED
- RDS_MULTI_AZ_SUPPORT
- RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- RDS_SNAPSHOT_ENCRYPTED
- RDS_SNAPSHOTS_PUBLIC_PROHIBITED
- RDS_STORAGE_ENCRYPTED
- REDSHIFT_BACKUP_ENABLED

Mots clés de règles AWS Config gérées pris en charge

- REDSHIFT_REQUIRE_TLS_SSL
- REDSHIFT_CLUSTER_CONFIGURATION_CHECK
- REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK
- REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK
- REDSHIFT_AUDIT_LOGGING_ENABLED
- REDSHIFT_CLUSTER_KMS_ENABLED
- REDSHIFT_DEFAULT_ADMIN_CHECK
- REDSHIFT_DEFAULT_DB_NAME_CHECK
- REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED
- ROOT_ACCOUNT_MFA_ENABLED
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC
- S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
- S3_BUCKET_ACL_PROHIBITED
- S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED
- S3_BUCKET_DEFAULT_LOCK_ENABLED
- S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED
- S3_BUCKET_LOGGING_ENABLED
- S3_BUCKET_POLICY_GRANTEE_CHECK
- S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE
- S3_BUCKET_PUBLIC_READ_PROHIBITED
- S3_BUCKET_PUBLIC_WRITE_PROHIBITED
- S3_BUCKET_REPLICATION_ENABLED
- S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED
- S3_BUCKET_SSL_REQUESTS_ONLY
- S3_BUCKET_VERSIONING_ENABLED
- S3_DEFAULT_ENCRYPTION_KMS

Mots clés de règles AWS Config gérées pris en charge

- S3_EVENT_NOTIFICATIONS_ENABLED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_LIFECYCLE_POLICY_CHECK
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- S3_VERSION_LIFECYCLE_POLICY_CHECK
- SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC
- SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED
- SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK
- SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS
- SECRETSMANAGER_ROTATION_ENABLED_CHECK
- SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK
- SECRETSMANAGER_SECRET_PERIODIC_ROTATION
- SECRETSMANAGER_SECRET_UNUSED
- SECRETSMANAGER_USING_CMK
- SECURITY_ACCOUNT_INFORMATION_PROVIDED
- SECURITYHUB_ENABLED
- SERVICE_VPC_ENDPOINT_ENABLED
- SES_MALWARE_SCANNING_ENABLED
- SHIELD_ADVANCED_ENABLED_AUTORENEW
- SHIELD_DRT_ACCESS
- SNS_ENCRYPTED_KMS
- SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED
- SSM_DOCUMENT_NOT_PUBLIC
- STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED
- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED

Mots clés de règles AWS Config gérées pris en charge

- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VPC_DEFAULT_SECURITY_GROUP_CLOSED
- VPC_FLOW_LOGS_ENABLED
- VPC_NETWORK_ACL_UNUSED_CHECK
- VPC_PEERING_DNS_RESOLUTION_CHECK
- VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS
- VPC_VPN_2_TUNNELS_UP
- WAF_CLASSIC_LOGGING_ENABLED
- WAF_GLOBAL_RULEGROUP_NOT_EMPTY
- WAF_GLOBAL_RULE_NOT_EMPTY
- WAF_GLOBAL_WEBACL_NOT_EMPT
- WAF_REGIONAL_RULEGROUP_NOT_EMPTY
- WAF_REGIONAL_RULE_NOT_EMPTY
- WAF_REGIONAL_WEBACL_NOT_EMPTY
- WAFV2_LOGGING_ENABLED
- WAFV2_RULEGROUP_NOT_EMPTY
- WAFV2_WEBACL_NOT_EMPTY

Utilisation de règles AWS Config personnalisées avec Audit Manager

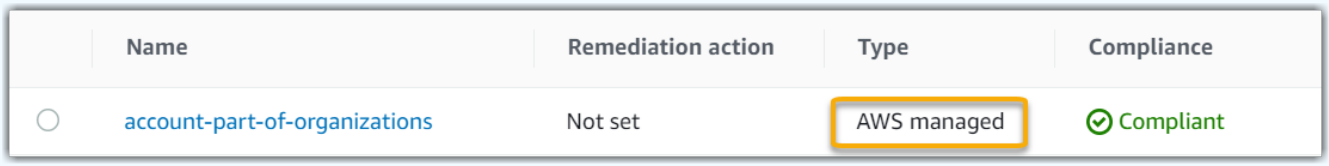
Vous pouvez désormais utiliser des règles AWS Config personnalisées comme source de données pour les rapports d'audit. Lorsqu'un contrôle possède une source de données mappée à une AWS Config règle, Audit Manager ajoute l'évaluation créée par la AWS Config règle.

Les règles personnalisées que vous pouvez utiliser dépendent de l'appareil avec Compte AWS lequel vous vous connectez à Audit Manager. Si vous pouvez accéder à une règle personnalisée dans AWS Config, vous pouvez l'utiliser comme mappage de source de données dans Audit Manager.

- Pour les particuliers Comptes AWS : vous pouvez utiliser n'importe laquelle des règles personnalisées que vous avez créées avec votre compte.

- Pour les comptes faisant partie d'une organisation : vous pouvez également utiliser n'importe laquelle de vos règles personnalisées au niveau des membres. Vous pouvez également utiliser n'importe laquelle des règles personnalisées mises à votre disposition au niveau dans AWS Config.

Pour obtenir des instructions sur la création d'un contrôle utilisant des règles personnalisées comme source de données, consultez les sections Création d'un nouveau contrôle à partir de zéro et Personnalisation d'un contrôle existant.

> **Tip**
>
> N'oubliez pas que les règles gérées ne figurent pas dans la liste déroulante des règles personnalisées d'Audit Manager.
> Pour vérifier si une AWS Config règle est une règle gérée ou personnalisée, vous pouvez le faire à l'aide de la AWS Config console. Dans le menu de navigation de gauche, choisissez Règles et recherchez la règle dans le tableau. S'il s'agit d'une règle gérée, la colonne Type indique géréeAWS .
>
> 
>
>
> Pour mapper une règle gérée en tant que source de données, vous pouvez rechercher le mot clé d'identification de la règle gérée dans Audit Manager dans la liste déroulante des règles gérées. Pour plus d'informations, consultez dans la section de résolution des problèmes.

Après avoir mappé vos règles personnalisées en tant que source de données pour un contrôle, vous pouvez associer ce contrôle à un framework personnalisé dans Audit Manager. Pour obtenir des instructions sur la façon de créer un framework personnalisé utilisant votre contrôle personnalisé, voir Création d'un nouveau framework à partir de zéro et Personnalisation d'un framework existant. Pour obtenir des instructions sur la façon d'ajouter votre contrôle à un framework personnalisé existant, consultez la section Modification d'un framework existant.

Pour plus d'informations sur la création d'une règle personnalisée dans AWS Config, consultez la section Développement d'une règle personnalisée pour AWS Config dans le Guide duAWS Config développeur.

Résolution des problèmes liés à AWS Config l'intégration avec Audit Manager

Pour trouver des réponses aux questions et problèmes courants, consultez la section relative à l'intégrationAWS Config dans la section Dépannage de ce guide.

AWS Security Hub commandes prises en charge par AWS Audit Manager

Audit Manager vous permet de communiquer les résultats des contrôles de conformité directement depuis Security Hub. Pour ce faire, vous devez définir un ou plusieurs contrôles Security Hub en tant que mappage de source de données lorsque vous configurez un contrôle personnalisé dans Audit Manager.

> **Note**
>
> - Audit Manager ne collecte pas de preuves à partir des AWS Config règles liées aux services créées par Security Hub. Pour plus d'informations, consultez dans la section de résolution des problèmes.
> - Le 9 novembre 2022, Security Hub a lancé des contrôles de sécurité automatisés conformes aux exigences de la version 1.4.0 du Center for Internet Security (CIS) AWS Foundations Benchmark, niveaux 1 et 2 (CIS v1.4.0). Dans Security Hub, la norme CIS v1.4.0 est prise en charge en plus de la norme CIS v1.2.0.

Rubriques

- Utilisation des contrôles Security Hub avec Audit Manager
- Contrôles Security Hub pris en charge

Utilisation des contrôles Security Hub avec Audit Manager

> **Tip**
>
> Nous vous recommandons d'activer le paramètre des résultats de contrôle consolidés dans Security Hub si ce n'est pas le cas. Si vous avez activé Security Hub depuis le 23 février 2003, ce paramètre est activé par défaut.

Lorsque les résultats consolidés sont activés, Security Hub produit un résultat unique pour chaque contrôle de sécurité (même lorsque le même contrôle s'applique à plusieurs normes). Chaque résultat du Security Hub est collecté dans le cadre d'une évaluation de ressource unique dans Audit Manager. Par conséquent, les résultats consolidés se traduisent par une diminution du nombre total d'évaluations uniques des ressources effectuées par Audit Manager pour les résultats de Security Hub. C'est pourquoi l'utilisation de résultats consolidés permet souvent de réduire les coûts d'utilisation de votre Audit Manager, sans pour autant sacrifier la qualité et la disponibilité des éléments probants. Pour plus d'informations sur la tarification, consultez Tarification d'AWS Audit Manager.

Exemples d'éléments probants lorsque les résultats consolidés sont activés ou désactivés

Les exemples suivants comparent la manière dont Audit Manager collecte et présente les éléments probants en fonction des paramètres de votre Security Hub.

When consolidated findings is turned on

Supposons que vous ayez activé les trois normes de sécurité suivantes dans Security Hub : AWS FSBP, PCI DSS et CIS Benchmark v1.2.0.

- Ces trois normes utilisent le même contrôle (IAM.4) avec la même AWS Config règle sous-jacente (iam-root-access-key-check).
- Le paramètre des résultats de contrôle consolidés étant activé, Security Hub génère un seul résultat pour ce contrôle.
- Security Hub envoie le résultat consolidé à Audit Manager pour ce contrôle.
- Les résultats consolidés constituent une évaluation des ressources unique dans Audit Manager. Par conséquent, un seul élément probant est ajouté à votre évaluation.

Voici un exemple de ce à quoi peuvent ressembler ces éléments probants :


```
{
    "SchemaVersion": "2018-10-08",
    "Id": "arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109",
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/securityhub",
    "ProductName": "Security Hub",
    "CompanyName": "AWS",
    "Region": "us-west-2",
    "GeneratorId": "security-control/IAM.4",
```

```
    "AwsAccountId": "111122223333",
    "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "FirstObservedAt": "2023-10-25T11:32:24.861Z",
    "LastObservedAt": "2023-11-02T11:59:19.546Z",
    "CreatedAt": "2023-10-25T11:32:24.861Z",
    "UpdatedAt": "2023-11-02T11:59:15.127Z",
    "Severity": {
        "Label": "INFORMATIONAL",
        "Normalized": 0,
        "Original": "INFORMATIONAL"
    },
    "Title": "IAM root user access key should not exist",
    "Description": "This AWS control checks whether the root user access key is
 available.",
    "Remediation": {
        "Recommendation": {
            "Text": "For information on how to correct this issue, consult the AWS
 Security Hub controls documentation.",
            "Url": "https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
        }
    },
    "ProductFields": {
        "RelatedAWSResources:0/name": "securityhub-iam-root-access-key-
check-000270f5",
        "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
        "aws/securityhub/ProductName": "Security Hub",
        "aws/securityhub/CompanyName": "AWS",
        "Resources:0/Id": "arn:aws:iam::111122223333:root",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/aws/
securityhub/arn:aws:securityhub:us-west-2:111122223333:security-control/IAM.4/
finding/09876543-p0o9-i8u7-y6t5-098765432109"
    },
    "Resources": [{
        "Type": "AwsAccount",
        "Id": "AWS::::Account:111122223333",
        "Partition": "aws",
        "Region": "us-west-2"
    }],
    "Compliance": {
        "Status": "PASSED",
        "RelatedRequirements": [
```

```
            "CIS AWS Foundations Benchmark v1.2.0/1.12"
        ],
        "SecurityControlId": "IAM.4",
        "AssociatedStandards": [{
                "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
            },
            {
                "StandardsId": "standards/aws-foundational-security-best-practices/
v/1.0.0"
            }
        ]
    },
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "RESOLVED"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "INFORMATIONAL",
            "Original": "INFORMATIONAL"
        },
        "Types": [
            "Software and Configuration Checks/Industry and Regulatory Standards"
        ]
    },
    "ProcessedAt": "2023-11-02T11:59:20.980Z"
}
```


When consolidated findings is turned off

Supposons que vous ayez activé les trois normes de sécurité suivantes dans Security Hub : AWS FSBP, PCI DSS et CIS Benchmark v1.2.0.

- Ces trois normes utilisent le même contrôle (IAM.4) avec la même AWS Config règle sous-jacente (iam-root-access-key-check).
- Le paramètre des résultats consolidés étant désactivé, Security Hub génère un résultat distinct par contrôle de sécurité pour chaque norme activée (dans ce cas, trois résultats).
- Security Hub envoie trois résultats distincts spécifiques à la norme à Audit Manager pour ce contrôle.

- Les trois résultats sont considérés comme trois évaluations de ressources uniques dans Audit Manager. En conséquence, trois éléments probants distincts sont ajoutés à votre évaluation.

Voici un exemple de ce à quoi peuvent ressembler ces éléments probants. Notez que dans cet exemple, chacune des trois charges utiles suivantes possède le même ID de contrôle de sécurité (*SecurityControlId":"IAM.4"*). Pour cette raison, le contrôle d'évaluation qui collecte ces éléments probants dans Audit Manager (IAM.4) reçoit trois éléments probants distincts lorsque les résultats suivants proviennent de Security Hub.

Élément probant pour la norme IAM.4 (FSBP)


```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/b5e68d5d-43c3-46c8-902d-51cb0d4da568"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"aws-foundational-security-best-practices/v/1.0.0/IAM.4",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
AWS-Foundational-Security-Best-Practices"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.848Z",
```

```
            "LastObservedAt":"2023-11-01T14:12:04.106Z",
            "CreatedAt":"2020-10-05T19:18:47.848Z",
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"IAM.4 IAM root user access key should not exist",
            "Description":"This AWS control checks whether the root user access key
 is available.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsArn":"arn:aws:securityhub:::standards/aws-foundational-
security-best-practices/v/1.0.0",
               "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0",
               "ControlId":"IAM.4",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/aws-foundational-security-best-practices/v/1.0.0/IAM.4",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
               "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/aws-
foundational-security-best-practices/v/1.0.0/IAM.4/finding/8e2e05a2-4d50-4c2e-
a78f-3cbe9402d17d"
            },
            "Resources":[
               {
                  "Type":"AwsAccount",
```

```
                "Id":"AWS::::Account:111122223333",
                "Partition":"aws",
                "Region":"us-west-2"
             }
          ],
          "Compliance":{
             "Status":"PASSED",
             "SecurityControlId":"IAM.4",
             "AssociatedStandards":[
                {
                   "StandardsId":"standards/aws-foundational-security-best-
practices/v/1.0.0"
                }
             ]
          },
          "WorkflowState":"NEW",
          "Workflow":{
             "Status":"RESOLVED"
          },
          "RecordState":"ACTIVE",
          "FindingProviderFields":{
             "Severity":{
                "Label":"INFORMATIONAL",
                "Original":"INFORMATIONAL"
             },
             "Types":[
                "Software and Configuration Checks/Industry and Regulatory
 Standards/AWS-Foundational-Security-Best-Practices"
             ]
          },
          "ProcessedAt":"2023-11-01T14:12:07.395Z"
       }
    ]
  }
}
```

Élément probant pour la norme IAM.4 (CIS 1.2)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
```

```
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
           "CompanyName":"AWS",
           "Region":"us-west-2",
           "GeneratorId":"arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0/rule/1.12",
           "AwsAccountId":"111122223333",
           "Types":[
              "Software and Configuration Checks/Industry and Regulatory Standards/
CIS AWS Foundations Benchmark"
           ],
           "FirstObservedAt":"2020-10-05T19:18:47.775Z",
           "LastObservedAt":"2023-11-01T14:12:07.989Z",
           "CreatedAt":"2020-10-05T19:18:47.775Z",
           "UpdatedAt":"2023-11-01T14:11:53.720Z",
           "Severity":{
              "Product":0,
              "Label":"INFORMATIONAL",
              "Normalized":0,
              "Original":"INFORMATIONAL"
           },
           "Title":"1.12 Ensure no root user access key exists",
           "Description":"The root user is the most privileged user in an AWS
 account. AWS Access Keys provide programmatic access to a given AWS account. It is
 recommended that all access keys associated with the root user be removed.",
           "Remediation":{
              "Recommendation":{
```

```
                "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
             }
          },
          "ProductFields":{
             "StandardsGuideArn":"arn:aws:securityhub:::ruleset/cis-aws-
foundations-benchmark/v/1.2.0",
             "StandardsGuideSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/cis-aws-foundations-benchmark/v/1.2.0",
             "RuleId":"1.12",
             "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
             "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
             "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
             "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/cis-aws-foundations-benchmark/v/1.2.0/1.12",
             "aws/securityhub/ProductName":"Security Hub",
             "aws/securityhub/CompanyName":"AWS",
             "Resources:0/Id":"arn:aws:iam::111122223333:root",
             "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/cis-aws-
foundations-benchmark/v/1.2.0/1.12/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
          },
          "Resources":[
             {
                "Type":"AwsAccount",
                "Id":"AWS::::Account:111122223333",
                "Partition":"aws",
                "Region":"us-west-2"
             }
          ],
          "Compliance":{
             "Status":"PASSED",
             "SecurityControlId":"IAM.4",
             "AssociatedStandards":[
                {
                   "StandardsId":"ruleset/cis-aws-foundations-benchmark/v/1.2.0"
                }
             ]
          },
          "WorkflowState":"NEW",
```

```
            "Workflow":{
               "Status":"RESOLVED"
            },
            "RecordState":"ACTIVE",
            "FindingProviderFields":{
               "Severity":{
                  "Label":"INFORMATIONAL",
                  "Original":"INFORMATIONAL"
               },
               "Types":[
                  "Software and Configuration Checks/Industry and Regulatory
 Standards/CIS AWS Foundations Benchmark"
               ]
            },
            "ProcessedAt":"2023-11-01T14:12:13.436Z"
         }
      ]
   }
}
```

Élément probant pour la norme PCI.IAM.1 (PCI DSS)

```
{
  "version":"0",
  "id":"12345678-1q2w-3e4r-5t6y-123456789012",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2023-10-27T18:55:59Z",
  "region":"us-west-2",
  "resources":[
     "arn:aws:securityhub:us-west-2::product/aws/securityhub/arn:aws:securityhub:us-
west-2:111122223333:subscription/aws-foundational-security-best-practices/v/1.0.0/
Lambda.1/finding/1dd8f2f8-cf1b-47c9-a875-8d7387fc9c23"
  ],
  "detail":{
     "findings":[
        {
           "SchemaVersion":"2018-10-08",
           "Id":"arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b",
           "ProductArn":"arn:aws:securityhub:us-west-2::product/aws/securityhub",
           "ProductName":"Security Hub",
```

```
            "CompanyName":"AWS",
            "Region":"us-west-2",
            "GeneratorId":"pci-dss/v/3.2.1/PCI.IAM.1",
            "AwsAccountId":"111122223333",
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory Standards/
PCI-DSS"
            ],
            "FirstObservedAt":"2020-10-05T19:18:47.788Z",
            "LastObservedAt":"2023-11-01T14:12:02.413Z",
            "CreatedAt":"2020-10-05T19:18:47.788Z",
            "UpdatedAt":"2023-11-01T14:11:53.720Z",
            "Severity":{
               "Product":0,
               "Label":"INFORMATIONAL",
               "Normalized":0,
               "Original":"INFORMATIONAL"
            },
            "Title":"PCI.IAM.1 IAM root user access key should not exist",
            "Description":"This AWS control checks whether the root user access key
 is available.",
            "Remediation":{
               "Recommendation":{
                  "Text":"For information on how to correct this issue, consult the
 AWS Security Hub controls documentation.",
                  "Url":"https://docs.aws.amazon.com/console/securityhub/IAM.4/
remediation"
               }
            },
            "ProductFields":{
               "StandardsArn":"arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
               "StandardsSubscriptionArn":"arn:aws:securityhub:us-
west-2:111122223333:subscription/pci-dss/v/3.2.1",
               "ControlId":"PCI.IAM.1",
               "RecommendationUrl":"https://docs.aws.amazon.com/console/securityhub/
IAM.4/remediation",
               "RelatedAWSResources:0/name":"securityhub-iam-root-access-key-
check-67cbb1c4",
               "RelatedAWSResources:0/type":"AWS::Config::ConfigRule",
               "StandardsControlArn":"arn:aws:securityhub:us-
west-2:111122223333:control/pci-dss/v/3.2.1/PCI.IAM.1",
               "aws/securityhub/ProductName":"Security Hub",
               "aws/securityhub/CompanyName":"AWS",
               "Resources:0/Id":"arn:aws:iam::111122223333:root",
```

```
            "aws/securityhub/FindingId":"arn:aws:securityhub:us-west-2::product/
aws/securityhub/arn:aws:securityhub:us-west-2:111122223333:subscription/pci-dss/
v/3.2.1/PCI.IAM.1/finding/3c75f651-6e2e-44f4-8e22-297d5c2d0c8b"
         },
         "Resources":[
            {
               "Type":"AwsAccount",
               "Id":"AWS::::Account:111122223333",
               "Partition":"aws",
               "Region":"us-west-2"
            }
         ],
         "Compliance":{
            "Status":"PASSED",
            "RelatedRequirements":[
               "PCI DSS 2.1",
               "PCI DSS 2.2",
               "PCI DSS 7.2.1"
            ],
            "SecurityControlId":"IAM.4",
            "AssociatedStandards":[
               {
                  "StandardsId":"standards/pci-dss/v/3.2.1"
               }
            ]
         },
         "WorkflowState":"NEW",
         "Workflow":{
            "Status":"RESOLVED"
         },
         "RecordState":"ACTIVE",
         "FindingProviderFields":{
            "Severity":{
               "Label":"INFORMATIONAL",
               "Original":"INFORMATIONAL"
            },
            "Types":[
               "Software and Configuration Checks/Industry and Regulatory
 Standards/PCI-DSS"
            ]
         },
         "ProcessedAt":"2023-11-01T14:12:05.950Z"
      }
   ]
```

```
  }
}
```

Contrôles Security Hub pris en charge

Les contrôles Security Hub suivants sont actuellement pris en charge par Audit Manager. Vous pouvez utiliser l'un des mots clés suivants d'ID de contrôle spécifiques à la norme lorsque vous configurez une source de données pour un contrôle personnalisé.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
CIS v1.2.0	1.2	IAM.5
CIS v1.2.0	1.3	IAM.8
CIS v1.2.0	1.4	IAM.3
CIS v1.2.0	1.5	IAM.11
CIS v1.2.0	1.6	IAM.12
CIS v1.2.0	1,7	IAM.13
CIS v1.2.0	1.8	IAM.14
CIS v1.2.0	1.9	IAM.15
CIS v1.2.0	1.10	IAM.16
CIS v1.2.0	1.11	IAM.17
CIS v1.2.0	1.12	IAM.4
CIS v1.2.0	1.13	IAM.9

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
CIS v1.2.0	1.14	IAM.6
CIS v1.2.0	1.16	IAM.2
CIS v1.2.0	1,20	IAM.18
CIS v1.2.0	1,22	IAM.1
CIS v1.2.0	2.1	CloudTrail1.
CIS v1.2.0	2.2	CloudTrail4.
CIS v1.2.0	2.3	CloudTrail6.
CIS v1.2.0	2,4	CloudTrail5.
CIS v1.2.0	2,5	Config.1
CIS v1.2.0	2.6	CloudTrail7.
CIS v1.2.0	2.7	CloudTrail2.
CIS v1.2.0	2,8	KMS.4
CIS v1.2.0	2.9	EC2.6
CIS v1.2.0	3.1	CloudWatch2.
CIS v1.2.0	3.2	CloudWatch3.
CIS v1.2.0	3.3	CloudWatch1.
CIS v1.2.0	3.4	CloudWatch4.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
CIS v1.2.0	3,5	CloudWatch5.
CIS v1.2.0	3.6	CloudWatch6.
CIS v1.2.0	3.7	CloudWatch7.
CIS v1.2.0	3.8	CloudWatch8.
CIS v1.2.0	3.9	CloudWatch9.
CIS v1.2.0	3,10	CloudWatch.10
CIS v1.2.0	3,11	CloudWatch.11
CIS v1.2.0	3,12	CloudWatch.12
CIS v1.2.0	3.13	CloudWatch.13
CIS v1.2.0	3,14	CloudWatch.14
CIS v1.2.0	4.1	EC2.13
CIS v1.2.0	4.2	EC2.14
CIS v1.2.0	4.3	EC2.2
PCI DSS	PCI. AutoScaling1.	AutoScaling1.
PCI DSS	PCI. CloudTrail1.	CloudTrail1.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
PCI DSS	PCI. CloudTrail2.	CloudTrail2.
PCI DSS	PCI. CloudTrail3.	CloudTrail3.
PCI DSS	PCI. CloudTrail4.	CloudTrail4.
PCI DSS	PCI. CodeBuild1.	CodeBuild1.
PCI DSS	PCI. CodeBuild2.	CodeBuild2.
PCI DSS	PCI.Config.1	Config.1
PCI DSS	PCI.CW.1	CloudWatch1.
PCI DSS	PCI.DMS.1	DMS.1
PCI DSS	PCI.EC2.1	EC2.1
PCI DSS	PCI.EC2.2	EC2.2
PCI DSS	PCI.EC2.3	EC2.3
PCI DSS	PCI.EC2.4	EC2,12
PCI DSS	PCI.EC2.5	EC2.13
PCI DSS	PCI.EC2.6	EC2.6

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
PCI DSS	PCI.ELBv2.1	ELB.1
PCI DSS	PCI.ES.1	ES.1
PCI DSS	PCI.ES.2	ES.2
PCI DSS	PCI. GuardDuty 1.	GuardDuty1.
PCI DSS	PCI.IAM.1	IAM.1
PCI DSS	PCI.IAM.2	IAM.2
PCI DSS	PCI.IAM.3	IAM.3
PCI DSS	PCI.IAM.4	IAM.4
PCI DSS	PCI.IAM.5	IAM.9
PCI DSS	PCI.IAM.6	IAM.6
PCI DSS	PCI.IAM.7	PCI.IAM.7
PCI DSS	PCI.IAM.8	PCI.IAM8.
PCI DSS	PCI.KMS.1	PCI.KMS.4
PCI DSS	PCI.Lambda.1	Lambda.1
PCI DSS	PCI.Lambda.2	Lambda.3
PCI DSS	PCI.Opens earch.1	Opensearch.1

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
PCI DSS	PCI.Opens earch.2	Opensearch.2
PCI DSS	PCI.RDS.1	RDS.1
PCI DSS	PCI.RDS.2	RDS.2
PCI DSS	PCI.Redshift.1	Redshift.1
PCI DSS	PCI.S3.1	S3.1
PCI DSS	PCI.S3.2	S3.2
PCI DSS	PCI.S3.3	S3.3
PCI DSS	PCI.S3.4	S3.4
PCI DSS	PCI.S3.5	S3.5
PCI DSS	PCI.S3.6	S3.1
PCI DSS	PCI. SageMaker 1.	SageMaker1.
PCI DSS	PCI.SSM.1	SSM.1
PCI DSS	PCI.SSM.2	SSM.2
PCI DSS	PCI.SSM.3	SSM.3
AWS Bonnes pratiques de sécurité fondamentales	Account.1	Account.1

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	Compte.2	Compte.2
AWS Bonnes pratiques de sécurité fondamentales	ACM.1	ACM.1
AWS Bonnes pratiques de sécurité fondamentales	ACM.2	ACM.2
AWS Bonnes pratiques de sécurité fondamentales	APIGateway.1	APIGateway.1
AWS Bonnes pratiques de sécurité fondamentales	APIGateway.2	APIGateway.2
AWS Bonnes pratiques de sécurité fondamentales	APIGateway.3	APIGateway.3
AWS Bonnes pratiques de sécurité fondamentales	APIGateway.4	APIGateway.4
AWS Bonnes pratiques de sécurité fondamentales	APIGateway.5	APIGateway.5
AWS Bonnes pratiques de sécurité fondamentales	APIGateway.8	APIGateway.8
AWS Bonnes pratiques de sécurité fondamentales	APIGateway.9	APIGateway.9

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	AppSync2.	AppSync2.
AWS Bonnes pratiques de sécurité fondamentales	AppSync5.	AppSync5.
AWS Bonnes pratiques de sécurité fondamentales	Athéna.1	Athéna.1
AWS Bonnes pratiques de sécurité fondamentales	AutoScaling1.	AutoScaling1.
AWS Bonnes pratiques de sécurité fondamentales	AutoScaling2.	AutoScaling2.
AWS Bonnes pratiques de sécurité fondamentales	AutoScaling3.	AutoScaling3.
AWS Bonnes pratiques de sécurité fondamentales	AutoScaling4.	AutoScaling4.
AWS Bonnes pratiques de sécurité fondamentales	Autoscaling.5	Autoscaling.5
AWS Bonnes pratiques de sécurité fondamentales	AutoScaling6.	AutoScaling6.
AWS Bonnes pratiques de sécurité fondamentales	AutoScaling9.	AutoScaling9.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	Sauvegarde.1	Sauvegarde.1
AWS Bonnes pratiques de sécurité fondamentales	CloudFormation1.	CloudFormation1.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront1.	CloudFront1.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront2.	CloudFront2.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront3.	CloudFront3.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront4.	CloudFront4.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront5.	CloudFront5.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront6.	CloudFront6.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront7.	CloudFront7.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront8.	CloudFront8.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	CloudFront9.	CloudFront9.
AWS Bonnes pratiques de sécurité fondamentales	CloudFront.10	CloudFront.10
AWS Bonnes pratiques de sécurité fondamentales	CloudFront.12	CloudFront.12
AWS Bonnes pratiques de sécurité fondamentales	CloudFront.13	CloudFront.13
AWS Bonnes pratiques de sécurité fondamentales	CloudTrail1.	CloudTrail1.
AWS Bonnes pratiques de sécurité fondamentales	CloudTrail2.	CloudTrail2.
AWS Bonnes pratiques de sécurité fondamentales	CloudTrail3.	CloudTrail3.
AWS Bonnes pratiques de sécurité fondamentales	CloudTrail4.	CloudTrail4.
AWS Bonnes pratiques de sécurité fondamentales	CloudTrail5.	CloudTrail5.
AWS Bonnes pratiques de sécurité fondamentales	CloudTrail6.	CloudTrail6.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	CloudTrail7.	CloudTrail7.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch1.	CloudWatch1.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch2.	CloudWatch2.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch3.	CloudWatch3.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch4.	CloudWatch4.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch5.	CloudWatch5.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch6.	CloudWatch6.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch7.	CloudWatch7.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch8.	CloudWatch8.
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch9.	CloudWatch9.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch.10	CloudWatch.10
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch.11	CloudWatch.11
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch.12	CloudWatch.12
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch.13	CloudWatch.13
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch.14	CloudWatch.14
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch.15	CloudWatch.15
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch.16	CloudWatch.16
AWS Bonnes pratiques de sécurité fondamentales	CloudWatch.17	CloudWatch.17
AWS Bonnes pratiques de sécurité fondamentales	CodeBuild1.	CodeBuild1.
AWS Bonnes pratiques de sécurité fondamentales	CodeBuild2.	CodeBuild2.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	CodeBuild3.	CodeBuild3.
AWS Bonnes pratiques de sécurité fondamentales	CodeBuild4.	CodeBuild4.
AWS Bonnes pratiques de sécurité fondamentales	CodeBuild5.	CodeBuild5.
AWS Bonnes pratiques de sécurité fondamentales	Config.1	Config.1
AWS Bonnes pratiques de sécurité fondamentales	DMS.1	DMS.1
AWS Bonnes pratiques de sécurité fondamentales	DMS.6	DMS.6
AWS Bonnes pratiques de sécurité fondamentales	DMS.7	DMS.7
AWS Bonnes pratiques de sécurité fondamentales	DMS.8	DMS.8
AWS Bonnes pratiques de sécurité fondamentales	DMS.9	DMS.9
AWS Bonnes pratiques de sécurité fondamentales	Document DB.1	Document DB.1

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	Document DB.2	Document DB.2
AWS Bonnes pratiques de sécurité fondamentales	Document DB.3	Document DB.3
AWS Bonnes pratiques de sécurité fondamentales	Document DB.4	Document DB.4
AWS Bonnes pratiques de sécurité fondamentales	Document DB.5	Document DB.5
AWS Bonnes pratiques de sécurité fondamentales	DynamoDB.1	DynamoDB.1
AWS Bonnes pratiques de sécurité fondamentales	DynamoDB.2	DynamoDB.2
AWS Bonnes pratiques de sécurité fondamentales	DynamoDB.3	DynamoDB.3
AWS Bonnes pratiques de sécurité fondamentales	Dynamo DB.4	Dynamo DB.4
AWS Bonnes pratiques de sécurité fondamentales	Dynamo DB.6	Dynamo DB.6
AWS Bonnes pratiques de sécurité fondamentales	EC2.1	EC2.1

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	EC2.2	EC2.2
AWS Bonnes pratiques de sécurité fondamentales	EC2.3	EC2.3
AWS Bonnes pratiques de sécurité fondamentales	EC2.4	EC2.4
AWS Bonnes pratiques de sécurité fondamentales	EC2.6	EC2.6
AWS Bonnes pratiques de sécurité fondamentales	EC2.7	EC2.7
AWS Bonnes pratiques de sécurité fondamentales	EC2.8	EC2.8
AWS Bonnes pratiques de sécurité fondamentales	EC2.9	EC2.9
AWS Bonnes pratiques de sécurité fondamentales	EC2.10	EC2.10
AWS Bonnes pratiques de sécurité fondamentales	EC2,12	EC2,12
AWS Bonnes pratiques de sécurité fondamentales	EC2.13	EC2.13

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	EC2.14	EC2.14
AWS Bonnes pratiques de sécurité fondamentales	EC2.15	EC2.15
AWS Bonnes pratiques de sécurité fondamentales	EC2.16	EC2.16
AWS Bonnes pratiques de sécurité fondamentales	EC2.17	EC2.17
AWS Bonnes pratiques de sécurité fondamentales	EC2.18	EC2.18
AWS Bonnes pratiques de sécurité fondamentales	EC2.19	EC2.19
AWS Bonnes pratiques de sécurité fondamentales	EC2.20	EC2.20
AWS Bonnes pratiques de sécurité fondamentales	EC2.21	EC2.21
AWS Bonnes pratiques de sécurité fondamentales	EC2.22	EC2.22
AWS Bonnes pratiques de sécurité fondamentales	EC2.23	EC2.23

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	EC2.24	EC2.24
AWS Bonnes pratiques de sécurité fondamentales	EC2.25	EC2.25
AWS Bonnes pratiques de sécurité fondamentales	EC2,28	EC2,28
AWS Bonnes pratiques de sécurité fondamentales	EC2,51	EC2,51
AWS Bonnes pratiques de sécurité fondamentales	ECR.1	ECR.1
AWS Bonnes pratiques de sécurité fondamentales	ECR.2	ECR.2
AWS Bonnes pratiques de sécurité fondamentales	ECR.3	ECR.3
AWS Bonnes pratiques de sécurité fondamentales	ECS.1	ECS.1
AWS Bonnes pratiques de sécurité fondamentales	ECS.2	ECS.2
AWS Bonnes pratiques de sécurité fondamentales	ECS.3	ECS.3

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	ECS.4	ECS.4
AWS Bonnes pratiques de sécurité fondamentales	ECS.5	ECS.5
AWS Bonnes pratiques de sécurité fondamentales	ECS.8	ECS.8
AWS Bonnes pratiques de sécurité fondamentales	ECS.9	ECS.9
AWS Bonnes pratiques de sécurité fondamentales	ECS.10	ECS.10
AWS Bonnes pratiques de sécurité fondamentales	ECS.12	ECS.12
AWS Bonnes pratiques de sécurité fondamentales	EFS.1	EFS.1
AWS Bonnes pratiques de sécurité fondamentales	EFS.2	EFS.2
AWS Bonnes pratiques de sécurité fondamentales	EFS.3	EFS.3
AWS Bonnes pratiques de sécurité fondamentales	EFS.4	EFS.4

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	EKS.1	EKS.1
AWS Bonnes pratiques de sécurité fondamentales	EKS.2	EKS.2
AWS Bonnes pratiques de sécurité fondamentales	EKS.8	EKS.8
AWS Bonnes pratiques de sécurité fondamentales	ElastiCache1.	ElastiCache1.
AWS Bonnes pratiques de sécurité fondamentales	ElastiCache2.	ElastiCache2.
AWS Bonnes pratiques de sécurité fondamentales	ElastiCache3.	ElastiCache3.
AWS Bonnes pratiques de sécurité fondamentales	ElastiCache4.	ElastiCache4.
AWS Bonnes pratiques de sécurité fondamentales	ElastiCache5.	ElastiCache5.
AWS Bonnes pratiques de sécurité fondamentales	ElastiCache6.	ElastiCache6.
AWS Bonnes pratiques de sécurité fondamentales	ElastiCache7.	ElastiCache7.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	ElasticBeanstalk1.	ElasticBeanstalk1.
AWS Bonnes pratiques de sécurité fondamentales	ElasticBeanstalk2.	ElasticBeanstalk2.
AWS Bonnes pratiques de sécurité fondamentales	ElasticBeanstalk3.	ElasticBeanstalk3.
AWS Bonnes pratiques de sécurité fondamentales	ELB.1	ELB.1
AWS Bonnes pratiques de sécurité fondamentales	ELB.2	ELB.2
AWS Bonnes pratiques de sécurité fondamentales	ELB.3	ELB.3
AWS Bonnes pratiques de sécurité fondamentales	ELB.4	ELB.4
AWS Bonnes pratiques de sécurité fondamentales	ELB.5	ELB.5
AWS Bonnes pratiques de sécurité fondamentales	ELB.6	ELB.6
AWS Bonnes pratiques de sécurité fondamentales	ELB.7	ELB.7

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	ELB.8	ELB.8
AWS Bonnes pratiques de sécurité fondamentales	ELB.9	ELB.9
AWS Bonnes pratiques de sécurité fondamentales	ELB.10	ELB.10
AWS Bonnes pratiques de sécurité fondamentales	ELB.12	ELB.12
AWS Bonnes pratiques de sécurité fondamentales	ELB.13	ELB.13
AWS Bonnes pratiques de sécurité fondamentales	ELB.14	ELB.14
AWS Bonnes pratiques de sécurité fondamentales	16 ELB	ELB.16
AWS Bonnes pratiques de sécurité fondamentales	ELBv2.1	ELB.1
AWS Bonnes pratiques de sécurité fondamentales	EMR.1	EMR.1
AWS Bonnes pratiques de sécurité fondamentales	EMR 2	EMR 2

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	ES.1	ES.1
AWS Bonnes pratiques de sécurité fondamentales	ES.2	ES.2
AWS Bonnes pratiques de sécurité fondamentales	ES.3	ES.3
AWS Bonnes pratiques de sécurité fondamentales	ES.4	ES.4
AWS Bonnes pratiques de sécurité fondamentales	ES.5	ES.5
AWS Bonnes pratiques de sécurité fondamentales	ES.6	ES.6
AWS Bonnes pratiques de sécurité fondamentales	ES.7	ES.7
AWS Bonnes pratiques de sécurité fondamentales	ES.8	ES.8
AWS Bonnes pratiques de sécurité fondamentales	EventBridge3.	EventBridge3.
AWS Bonnes pratiques de sécurité fondamentales	EventBridge4.	EventBridge4.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	FSx.1	FSx.1
AWS Bonnes pratiques de sécurité fondamentales	GuardDuty1.	GuardDuty1.
AWS Bonnes pratiques de sécurité fondamentales	IAM.1	IAM.1
AWS Bonnes pratiques de sécurité fondamentales	IAM.2	IAM.2
AWS Bonnes pratiques de sécurité fondamentales	IAM.3	IAM.3
AWS Bonnes pratiques de sécurité fondamentales	IAM.4	IAM.4
AWS Bonnes pratiques de sécurité fondamentales	IAM.5	IAM.5
AWS Bonnes pratiques de sécurité fondamentales	IAM.6	IAM.6
AWS Bonnes pratiques de sécurité fondamentales	IAM.7	IAM.7
AWS Bonnes pratiques de sécurité fondamentales	IAM.8	IAM.8

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	IAM.9	IAM.9
AWS Bonnes pratiques de sécurité fondamentales	IAM.10	JE SUIS 10
AWS Bonnes pratiques de sécurité fondamentales	IAM.11	IAM.11
AWS Bonnes pratiques de sécurité fondamentales	IAM.12	IAM.12
AWS Bonnes pratiques de sécurité fondamentales	IAM.13	IAM.13
AWS Bonnes pratiques de sécurité fondamentales	IAM.14	IAM.14
AWS Bonnes pratiques de sécurité fondamentales	IAM.15	IAM.15
AWS Bonnes pratiques de sécurité fondamentales	IAM.16	IAM.16
AWS Bonnes pratiques de sécurité fondamentales	IAM.17	IAM.17
AWS Bonnes pratiques de sécurité fondamentales	IAM.18	IAM.18

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	JE SUIS 19	JE SUIS 19
AWS Bonnes pratiques de sécurité fondamentales	IAM.21	IAM.21
AWS Bonnes pratiques de sécurité fondamentales	IAM.22	JE SUIS 22
AWS Bonnes pratiques de sécurité fondamentales	Kinesis.1	Kinesis.1
AWS Bonnes pratiques de sécurité fondamentales	KMS.1	KMS.1
AWS Bonnes pratiques de sécurité fondamentales	KMS.2	KMS.2
AWS Bonnes pratiques de sécurité fondamentales	KMS.3	KMS.3
AWS Bonnes pratiques de sécurité fondamentales	KMS.4	KMS.4
AWS Bonnes pratiques de sécurité fondamentales	Lambda.1	Lambda.1
AWS Bonnes pratiques de sécurité fondamentales	Lambda.2	Lambda.2

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	Lambda.3	Lambda.3
AWS Bonnes pratiques de sécurité fondamentales	Lambda.5	Lambda.5
AWS Bonnes pratiques de sécurité fondamentales	Macie.1	Macie.1
AWS Bonnes pratiques de sécurité fondamentales	MQ.5	MQ.5
AWS Bonnes pratiques de sécurité fondamentales	MQ.6	MQ.6
AWS Bonnes pratiques de sécurité fondamentales	MSK.1	MSK 1
AWS Bonnes pratiques de sécurité fondamentales	MASQUE 2	MSK 2
AWS Bonnes pratiques de sécurité fondamentales	Neptune.1	Neptune.1
AWS Bonnes pratiques de sécurité fondamentales	Neptune.2	Neptune.2
AWS Bonnes pratiques de sécurité fondamentales	Neptune.3	Neptune.3

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	Neptune.4	Neptune.4
AWS Bonnes pratiques de sécurité fondamentales	Neptune.5	Neptune.5
AWS Bonnes pratiques de sécurité fondamentales	Neptune.6	Neptune.6
AWS Bonnes pratiques de sécurité fondamentales	Neptune.7	Neptune.7
AWS Bonnes pratiques de sécurité fondamentales	Neptune.8	Neptune.8
AWS Bonnes pratiques de sécurité fondamentales	Neptune.9	Neptune.9
AWS Bonnes pratiques de sécurité fondamentales	NetworkFirewall1.	NetworkFirewall1.
AWS Bonnes pratiques de sécurité fondamentales	NetworkFirewall2.	NetworkFirewall2.
AWS Bonnes pratiques de sécurité fondamentales	NetworkFirewall3.	NetworkFirewall3.
AWS Bonnes pratiques de sécurité fondamentales	NetworkFirewall4.	NetworkFirewall4.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	NetworkFirewall5.	NetworkFirewall5.
AWS Bonnes pratiques de sécurité fondamentales	NetworkFirewall6.	NetworkFirewall6.
AWS Bonnes pratiques de sécurité fondamentales	NetworkFirewall9.	NetworkFirewall9.
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.1	Opensearch.1
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.2	Opensearch.2
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.3	Opensearch.3
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.4	Opensearch.4
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.5	Opensearch.5
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.6	Opensearch.6
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.7	Opensearch.7

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.8	Opensearch.8
AWS Bonnes pratiques de sécurité fondamentales	Opensearch.10	Opensearch.10
AWS Bonnes pratiques de sécurité fondamentales	PCA.1	PCA.1
AWS Bonnes pratiques de sécurité fondamentales	RDS.1	RDS.1
AWS Bonnes pratiques de sécurité fondamentales	RDS.2	RDS.2
AWS Bonnes pratiques de sécurité fondamentales	RDS.3	RDS.3
AWS Bonnes pratiques de sécurité fondamentales	RDS.4	RDS.4
AWS Bonnes pratiques de sécurité fondamentales	RDS.5	RDS.5
AWS Bonnes pratiques de sécurité fondamentales	RDS.6	RDS.6
AWS Bonnes pratiques de sécurité fondamentales	RDS.7	RDS.7

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	RDS.8	RDS.8
AWS Bonnes pratiques de sécurité fondamentales	RDS.9	RDS.9
AWS Bonnes pratiques de sécurité fondamentales	RDS.10	RDS.10
AWS Bonnes pratiques de sécurité fondamentales	RDS.11	RDS.11
AWS Bonnes pratiques de sécurité fondamentales	RDS.12	RDS.12
AWS Bonnes pratiques de sécurité fondamentales	RDS.13	RDS.13
AWS Bonnes pratiques de sécurité fondamentales	RDS.14	RDS.14
AWS Bonnes pratiques de sécurité fondamentales	RDS.15	RDS.15
AWS Bonnes pratiques de sécurité fondamentales	RDS.16	RDS.16
AWS Bonnes pratiques de sécurité fondamentales	RDS.17	RDS.17

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	RDS.18	RDS.18
AWS Bonnes pratiques de sécurité fondamentales	RDS.19	RDS.19
AWS Bonnes pratiques de sécurité fondamentales	RDS.20	RDS.20
AWS Bonnes pratiques de sécurité fondamentales	RDS.21	RDS.21
AWS Bonnes pratiques de sécurité fondamentales	RDS.22	RDS.22
AWS Bonnes pratiques de sécurité fondamentales	RDS.23	RDS.23
AWS Bonnes pratiques de sécurité fondamentales	RDS.24	RDS.24
AWS Bonnes pratiques de sécurité fondamentales	RDS.25	RDS.25
AWS Bonnes pratiques de sécurité fondamentales	RDS.26	RDS.26
AWS Bonnes pratiques de sécurité fondamentales	RDS.27	RDS.27

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	RDS.34	RDS.34
AWS Bonnes pratiques de sécurité fondamentales	RDS.35	RDS.35
AWS Bonnes pratiques de sécurité fondamentales	Redshift.1	Redshift.1
AWS Bonnes pratiques de sécurité fondamentales	Redshift.2	Redshift.2
AWS Bonnes pratiques de sécurité fondamentales	Redshift.3	Redshift.3
AWS Bonnes pratiques de sécurité fondamentales	Redshift.4	Redshift.4
AWS Bonnes pratiques de sécurité fondamentales	Redshift.6	Redshift.6
AWS Bonnes pratiques de sécurité fondamentales	Redshift.7	Redshift.7
AWS Bonnes pratiques de sécurité fondamentales	Redshift.8	Redshift.8
AWS Bonnes pratiques de sécurité fondamentales	Redshift.9	Redshift.9

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	Redshift.10	Redshift.10
AWS Bonnes pratiques de sécurité fondamentales	Itinéraire 53.2	Itinéraire 53.2
AWS Bonnes pratiques de sécurité fondamentales	S3.1	S3.1
AWS Bonnes pratiques de sécurité fondamentales	S3.2	S3.2
AWS Bonnes pratiques de sécurité fondamentales	S3.3	S3.3
AWS Bonnes pratiques de sécurité fondamentales	S3.4	S3.4
AWS Bonnes pratiques de sécurité fondamentales	S3.5	S3.5
AWS Bonnes pratiques de sécurité fondamentales	S3.6	S3.6
AWS Bonnes pratiques de sécurité fondamentales	S3,7	S3.7
AWS Bonnes pratiques de sécurité fondamentales	S3.8	S3.8

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	S3.9	S3.9
AWS Bonnes pratiques de sécurité fondamentales	S3.11	S3.11
AWS Bonnes pratiques de sécurité fondamentales	S3.12	S3.12
AWS Bonnes pratiques de sécurité fondamentales	S3.13	S3.13
AWS Bonnes pratiques de sécurité fondamentales	S3,14	S3,14
AWS Bonnes pratiques de sécurité fondamentales	S3,15	S3,15
AWS Bonnes pratiques de sécurité fondamentales	S3.17	S3.17
AWS Bonnes pratiques de sécurité fondamentales	S3,19	S3,19
AWS Bonnes pratiques de sécurité fondamentales	S3,19	S3,20
AWS Bonnes pratiques de sécurité fondamentales	SageMaker1.	SageMaker1.

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques de sécurité fondamentales	SageMaker2.	SageMaker2.
AWS Bonnes pratiques de sécurité fondamentales	SageMaker3.	SageMaker3.
AWS Bonnes pratiques de sécurité fondamentales	SecretsManager1.	SecretsManager1.
AWS Bonnes pratiques fondamentales en matière de sécurité	SecretsManager2.	SecretsManager2.
AWS Bonnes pratiques fondamentales en matière de sécurité	SecretsManager3.	SecretsManager3.
AWS Bonnes pratiques fondamentales en matière de sécurité	SecretsManager4.	SecretsManager4.
AWS Bonnes pratiques fondamentales en matière de sécurité	SNS.1	SNS.1
AWS Bonnes pratiques fondamentales en matière de sécurité	SNS.2	SNS.2
AWS Bonnes pratiques fondamentales en matière de sécurité	SQS.1	SQS.1
AWS Bonnes pratiques fondamentales en matière de sécurité	SSM.1	SSM.1

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques fondamentales en matière de sécurité	SSM.2	SSM.2
AWS Bonnes pratiques fondamentales en matière de sécurité	SSM.3	SSM.3
AWS Bonnes pratiques fondamentales en matière de sécurité	SSM.4	SSM.4
AWS Bonnes pratiques fondamentales en matière de sécurité	StepFunctions1.	StepFunctions1.
AWS Bonnes pratiques fondamentales en matière de sécurité	WAF.1	WAF.1
AWS Bonnes pratiques fondamentales en matière de sécurité	WAF.2	WAF.2
AWS Bonnes pratiques fondamentales en matière de sécurité	WAF.3	WAF.3
AWS Bonnes pratiques fondamentales en matière de sécurité	WAF.4	WAF.4
AWS Bonnes pratiques fondamentales en matière de sécurité	WAF.6	WAF.6
AWS Bonnes pratiques fondamentales en matière de sécurité	WAF.7	WAF.7

Norme de sécurité	Mot-clé pris en charge dans Audit Manager (ID de contrôle standard dans Security Hub)	Documentation associée au contrôle (ID de contrôle de sécurité correspondant dans Security Hub)
AWS Bonnes pratiques fondamentales en matière de sécurité	WAF.8	WAF.8
AWS Bonnes pratiques fondamentales en matière de sécurité	WAF.10	WAF.10
AWS Bonnes pratiques fondamentales en matière de sécurité	WAF.11	WAF.11
AWS Bonnes pratiques fondamentales en matière de sécurité	WAF.12	WAF.12

Appels d'API pris en charge par AWS Audit Manager

Audit Manager effectue des appels d'API Services AWS pour collecter un instantané des détails de configuration de vos AWS ressources. Vous pouvez spécifier ces appels d'API en tant que mappage de source de données lorsque vous configurez un contrôle personnalisé dans Audit Manager.

Pour chaque ressource faisant l'objet d'un appel d'API, Audit Manager capture un instantané de configuration et le convertit en éléments probants. Cela se traduit par un élément probant par ressource, par opposition à un élément probant par appel d'API.

Par exemple, si l'appel d'API `ec2_DescribeRouteTables` capture des instantanés de configuration à partir de cinq tables de routage, vous obtiendrez cinq éléments probants au total pour cet appel d'API unique. Chaque élément probant est un instantané de la configuration d'une table de routage individuelle.

Sur cette page

- Appels d'API pris en charge pour les sources de données de contrôle personnalisées
- Appels d'API paginés

- Appels d'API utilisés dans le cadre standard AWS License Manager

Appels d'API pris en charge pour les sources de données de contrôle personnalisées

Dans vos contrôles personnalisés, vous pouvez utiliser l'un des appels d'API suivants comme source de données. Audit Manager peut ensuite utiliser ces appels d'API pour collecter des preuves concernant votre AWS utilisation.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
acm_ GetAccountConfiguration	Collectez un instantané des options de configuration de compte associées à votre Compte AWS.
acm_ ListCertificates	Récupérez une liste des ARN de certificat et des noms de domaine.
cloudtrail_ DescribeTrails	Collectez un instantané des paramètres d'un ou de plusieurs journaux d'activité associés à la région actuelle de votre Compte AWS.
cloudwatch_ DescribeAlarms	Collectez un instantané de la configuration des alarmes utilisées pour votre Compte AWS.
configuration_ DescribeConfigRules	Récupérez les détails de vos AWS Config règles.
configuration_ DescribeDeliveryChannels	Collectez un instantané de la configuration des canaux de diffusion de votre Compte AWS.
connexion directe_ DescribeDirectConnectGateways	Récupérez la liste de toutes vos AWS Direct Connect passerelles.
connexion directe_ DescribeVirtualGateways	Récupérez la liste des passerelles privées virtuelles appartenant à votre Compte AWS.
docdb_ DescribeCertificates	Collectez une liste des certificats de votre Compte AWS.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
DocDB_DescribeDB ClusterParameterGroups	Collectez une liste des descriptions `DBClusterParameter Group` de votre Compte AWS.
docdb_DescribeDBInstances	Collectez des informations sur les instances Amazon DynamoDB provisionnées de votre Compte AWS.
dynamodb_ DescribeTable	Collectez des instantanés de la configuration des tables DynamoDB de votre Compte AWS. Lorsque vous utilisez cette API comme source de données, il n'est pas nécessaire de fournir le nom d'une table DynamoDB spécifique. Audit Manager utilise plutôt l'opération `ListTables` pour répertorier toutes vos tables. Pour chaque table répertoriée, Audit Manager effectue ensuite l'opération `DescribeTable` pour générer des éléments probants pour cette ressource.
dynamodb_ ListBackups	Récupérez la liste des sauvegardes DynamoDB associées à votre Compte AWS.
dynamodb_ ListGlobalTables	Récupérez la liste de l'ensemble des tables globales se trouvant actuellement dans votre Compte AWS.
dynamodb_ ListTables	Récupérez une liste de l'ensemble des noms de table associés à votre Compte AWS et à votre point de terminaison actuel.
ec2_ DescribeAddresses	Collectez un instantané de vos adresses IP Elastic.
ec2_ DescribeCustomerGa teways	Collectez un instantané de vos passerelles clients de VPN.
ec2_ DescribeEgressOnly InternetGateways	Collectez un instantané de vos passerelles Internet de sortie uniquement.
ec2_ DescribeFlowLogs	Collectez un instantané de vos journaux de flux.
ec2_ DescribeInstances	Collectez un instantané de vos instances.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
ec2_ DescribeInternetGateways	Collectez un instantané de vos passerelles Internet.
ec2_ DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	Collectez une description des associations entre les groupes d'interfaces virtuelles et les tables de routage des passerelles locales dans votre Compte AWS.
ec2_ DescribeLocalGateways	Collectez un instantané de vos passerelles locales.
ec2_ DescribeLocalGatewayVirtualInterfaces	Collectez un instantané de vos interfaces virtuelles de passerelle locale.
ec2_ DescribeNatGateways	Collectez un instantané de vos passerelles NAT.
ec2_ DescribeNetworkAcls	Collectez un instantané de vos ACL réseau.
ec2_ DescribeRouteTables	Collectez un instantané de vos tables de routage.
ec2_ DescribeSecurityGroups	Collectez un instantané de vos groupes de sécurité.
ec2_ DescribeTransitGateways	Collectez un instantané de vos passerelles de transit.
ec2_ DescribeVolumes	Collectez un instantané de vos points de terminaison de VPC.
ec2_ DescribeVpcs	Collectez un instantané de vos VPC.
ec2_ DescribeVpcEndpoints	Collectez un instantané de vos points de terminaison de VPC.
ec2_ DescribeVpcPeeringConnections	Collectez un instantané de vos connexions VPN.
ec2_ DescribeVpnConnections	Collectez un instantané de vos connexions VPN.
ec2_ DescribeVpnGateways	Collectez un instantané de vos passerelles privées virtuelles.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
ec2_ GetEbsDefaultKmsKeyId	Collectez un instantané du chiffrement EBS par défaut AWS KMS key pour votre Compte AWS région actuelle.
ec2_ GetEbsEncryptionBy Default	Indique si le chiffrement EBS par défaut est activé pour votre Compte AWS dans la région actuelle.
ecs_ DescribeClusters	Collectez un instantané de vos clusters ECS.
eks_ DescribeAddonVersions	Collectez un instantané des versions de vos add-on.
elasticache_ DescribeC acheClusters	Collectez un instantané de vos clusters provisionnés.
elasticache_ DescribeS erviceUpdates	Collectez un instantané des mises à jour de service pour Amazon ElastiCache.
système de fichiers élastique_ DescribeAccessPoints	Collectez un instantané des points d'accès Amazon EFS de votre Compte AWS.
système de fichiers élastique_ DescribeFileSystems	Collectez un instantané de vos systèmes de fichiers Amazon EFS.
équilibrage de charge élastique v2_ DescribeL oadBalancers	Collectez un instantané des équilibreurs de charge de votre Compte AWS.
elasticloadbalancingv2_Desc ribeSSLPolicies	Collectez un instantané des politiques que vous utilisez pour la négociation SSL.
équilibrage de charge élastique v2_ DescribeT argetGroups	Collectez un instantané de vos groupes cibles ELB.
elasticmapreduce_ ListSecur ityConfigurations	Récupérez la liste des configurations de sécurité visibles par votre Compte AWS, ainsi que leurs noms, dates et heures de création.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
événements_ ListConnections	Récupérez la liste des EventBridge connexions Amazon dans votre Compte AWS.
événements_ ListEventBuses	Récupérez la liste des bus d' EventBridge événements Amazon présents dans votre répertoire Compte AWS, y compris le bus d'événements par défaut, les bus d'événements personnalisés et les bus d'événements partenaires.
événements_ ListEvent Sources	Récupérez une liste des sources d'événement partenaire partagées avec votre Compte AWS.
événements_ ListRules	Récupérez la liste de vos EventBridge règles Amazon.
tuyau d'incendi_ ListDeliv eryStreams	Récupérez la liste de vos flux de diffusion.
fsx_ DescribeFileSystems	Collectez un instantané des systèmes de fichiers appartenant à votre Compte AWS.
devoir de guard_ ListDetec tors	Récupérez une liste des ressources `detectorIds` pour votre GuardDuty détecteur Amazon.
iam_ GenerateCredential Report	Générez un rapport d'informations d'identification pour votre Compte AWS.
iam_ GetAccountPassword Policy	Collectez un instantané de la politique de mot de passe de votre Compte AWS.
iam_ GetAccountSummary	Collectez un instantané de l'utilisation des entités et des quotas IAM dans votre Compte AWS.
iam_ ListGroupPolicies	Récupérez la liste des politiques intégrées intégrées dans un groupe IAM disponible dans votre. Compte AWS
iam_ ListGroups	Récupérez la liste des groupes IAM associés à un préfixe de chemin disponible dans votre. Compte AWS

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
Identifiant iam_ ListOpen ConnectProviders	Récupérez la liste des objets de ressource de fournisseur OpenID Connect (OIDC) IAM définis dans votre Compte AWS.
iam_ ListPolicies	Récupérez la liste de toutes les politiques gérées disponibl es dans votre Compte AWS, y compris vos propres politiques gérées définies par le client et l'ensemble des politiques gérées par AWS.
iam_ ListRoles	Récupérez la liste des rôles IAM associés à un préfixe de chemin disponible dans votre. Compte AWS
iam_ListSAMLProviders	Récupérez la liste des objets de ressource de fournisseur SAML définis dans IAM de votre Compte AWS.
iam_ ListUsers	Récupérez la liste des utilisateurs IAM de votre Compte AWS.
Appareils iam_ MFA ListVirtu al	Récupérez la liste des périphériques MFA virtuels définis dans votre Compte AWS.
kafka_ ListClusters	Récupérez la liste des clusters Amazon MSK présents dans votre Compte AWS.
kafka_ ListKafkaVersions	Récupérez la liste des objets de version Apache Kafka de votre Compte AWS.
kinésie_ ListStreams	Récupérez la liste de vos flux de données Kinesis.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
kms_ GetKeyPolicy	Audit Manager utilise cette API pour collecter un instantané des stratégies de clé pour votre AWS KMS keys de votre Compte AWS. Lorsque vous utilisez cette API comme source de données, il n'est pas nécessaire de fournir le nom d'une source spécifique AWS KMS key. Audit Manager utilise plutôt l'opération `ListKeys` pour répertorier toutes vos clés KMS. Pour chaque clé KMS répertoriée, Audit Manager effectue ensuite l'opération `GetKeyPolicy` pour générer des éléments probants pour cette ressource.
kms_ GetKeyRotationStatus	Audit Manager utilise cette API pour déterminer si la rotation automatique est activée AWS KMS keys dans votre Compte AWS. Lorsque vous utilisez cette API comme source de données, il n'est pas nécessaire de fournir le nom d'une source spécifique AWS KMS key. Audit Manager utilise plutôt l'opération `ListKeys` pour répertorier toutes vos clés KMS. Pour chaque clé KMS répertoriée, Audit Manager effectue ensuite l'opération `GetKeyRotationStatus` pour générer des éléments probants pour cette ressource.
kms_ ListKeys	Récupérez une liste des AWS KMS keys dans votre Compte AWS.
lambda_ ListFunctions	Récupérez la liste des fonctions Lambda de votre ordinateur Compte AWS, avec la configuration spécifique à chaque version.
rds_DescribeDBClusters	Collectez un instantané des clusters de base de données Amazon Aurora et des clusters de base de données multi-AZ existants dans votre Compte AWS.

Appel d'API pris en charge	Comment Audit Manager utilise cette API pour collecter des preuves
rds_DescribeDBInstances	Collectez un instantané des instances RDS provisionnées de votre Compte AWS.
redshift_ DescribeClusters	Collectez un instantané des clusters Amazon Redshift provisionnés de votre Compte AWS.
s3_ GetBucketEncryption	Collectez un instantané indiquant la configuration de chiffrement par défaut pour vos compartiments S3. Lorsque vous utilisez cette API comme source de données, il n'est pas nécessaire de fournir le nom d'un compartiment S3 spécifique. Audit Manager utilise plutôt l'opération `ListBuckets` pour répertorier tous vos compartiments. Pour chaque compartiment répertorié, Audit Manager effectue ensuite l'opération `GetBucketEncryption` pour générer des éléments probants pour cette ressource. Audit Manager peut uniquement fournir l'état de chiffrement pour les buckets créés en même temps Région AWS que votre évaluation. Si vous avez besoin de connaître l'état de chiffrement de tous vos compartiments S3 sur plusieurs Régions AWS, nous vous recommandons de créer une évaluation pour chacun des compartiments Région AWS où vous possédez un compartiment S3.
s3_ ListBuckets	Récupérez la liste des compartiments S3 de votre Compte AWS.
sns_ ListTopics	Récupérez une liste des rubriques SNS dans votre Compte AWS.
sqs_ ListQueues	Récupérez la liste des files d'attente SQS de votre. Compte AWS

Appels d'API paginés

Beaucoup Services AWS collectent et stockent de grandes quantités de données. Par conséquent, lorsqu'un appel d'API `list`, `describe` ou `get` tente de renvoyer vos données, les résultats peuvent être nombreux. Si la quantité de données est trop importante pour être renvoyée en une seule réponse, les résultats peuvent être divisés en éléments plus faciles à gérer grâce à la pagination. Cela divise les résultats en « pages » de données, ce qui facilite la gestion des réponses.

Certains des appels d'API pris en charge par Audit Manager sont paginés. Cela signifie qu'ils renvoient des résultats partiels dans un premier temps et nécessitent des demandes ultérieures pour renvoyer l'ensemble de résultats complet. Par exemple, l'opération DescribeDBInstances d'Amazon RDS renvoie jusqu'à 100 instances à la fois, et les demandes suivantes sont nécessaires pour renvoyer la page de résultats suivante.

Depuis le 8 mars 2023, Audit Manager prend en charge les appels d'API paginés en tant que source de données pour la collecte d'éléments probants. Auparavant, si un appel d'API paginé était utilisé comme source de données, seul un sous-ensemble de vos ressources était renvoyé dans la réponse de l'API (jusqu'à 100 résultats). Audit Manager appelle désormais l'opération d'API paginée à plusieurs reprises et obtient chaque page de résultats jusqu'à ce que toutes les ressources soient renvoyées. Pour chaque ressource, Audit Manager capture ensuite un instantané de configuration et l'enregistre comme élément probant. Étant donné que l'ensemble complet de vos ressources est désormais capturé dans la réponse de l'API, il est probable que vous remarquiez une augmentation du nombre d'éléments probants collectés.

Audit Manager gère automatiquement la pagination des appels d'API pour vous. Si vous créez un contrôle personnalisé qui utilise un appel d'API paginé comme source de données, vous n'avez pas besoin de définir des paramètres de pagination.

Appels d'API utilisés dans le cadre standard AWS License Manager

Dans le cadre standard AWS License Manager, Audit Manager utilise une activité personnalisée appelée `GetLicenseManagerSummary` pour collecter des éléments probants. Cette activité fait appel aux trois API du gestionnaire de licences suivantes :

- ListLicenseConfigurations
- ListAssociationsForLicenseConfiguration
- ListUsageForLicenseConfiguration

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

Exemple

Supposons que vous utilisiez deux produits sous licence (SQL Service 2017 et Oracle Database Enterprise Edition). Tout d'abord, l'`GetLicenseManagerSummary`activité appelle l'ListLicenseConfigurationsAPI, qui fournit des détails sur les configurations de licence de votre compte. Ensuite, il ajoute des données contextuelles supplémentaires pour chaque configuration de licence en appelant ListUsageForLicenseConfigurationet ListAssociationsForLicenseConfiguration. Enfin, elle convertit les données de configuration de licence en éléments probants et les associe aux contrôles respectifs du framework (4.5 - Licence gérée par le client pour SQL Server 2017 et 3.0.4 - Licence gérée par le client pour Oracle Database Enterprise Edition).

Si vous utilisez un produit sous licence qui n'est couvert par aucun des contrôles du framework, ces données de configuration de licence sont jointes en tant qu'élément probant au contrôle suivant : 5.0 - Licence gérée par le client pour les autres licences.

AWS CloudTrail noms d'événements pris en charge par AWS Audit Manager

Vous pouvez saisir les événements AWS CloudTrail de gestion et les événements de service globaux à titre de preuve dans Audit Manager. Pour ce faire, vous devez spécifier le nom de l' CloudTrail événement en tant que mot-clé de mappage de source de données lorsque vous créez un contrôle personnalisé.

> **Note**
>
> Audit Manager capture uniquement les événements de gestion et les événements de service mondiaux. Les événements liés aux données et les événements d'analyse ne sont pas disponibles en tant qu'éléments probants. Pour plus d'informations sur les différents types d' CloudTrail événements, consultez les CloudTrail concepts du guide de l'AWS CloudTrail utilisateur.

Par exception à ce qui précède, les CloudTrail événements suivants ne sont pas pris en charge par Audit Manager :

- kms_ GenerateDataKey

- kms_Decrypt
- sts_ AssumeRole
- kinesisvideo_ GetDataEndpoint
- kinesisvideo_ GetSignalingChannelEndpoint
- kinesisvideo_ DescribeSignalingChannel
- kinesisvideo_ DescribeStream

Depuis le 11 mai 2023, Audit Manager ne prend plus en charge les CloudTrail événements en lecture seule en tant que mots clés pour la collecte de preuves. Nous avons supprimé un total de 3 135 mots clés en lecture seule. Dans la mesure où les clients et Services AWS passent des appels en lecture aux API, les événements en lecture seule sont bruyants. Par conséquent, les mots clés en lecture seule collectent de nombreux éléments probants qui ne sont ni fiables ni pertinents pour les audits. Les mots clés en lecture seule incluent `ListDescribe`, et les appels `Get` d'API (par exemple, GetObjectet ListBucketspour Amazon S3). Si vous utilisiez l'un de ces mots clés pour recueillir des éléments probants, aucune action n'est requise. Les mots clés ont été automatiquement supprimés de la console Audit Manager et de vos évaluations, et aucun élément probant n'est collectée pour ces mots clés.

Paramètres AWS Audit Manager

Vous pouvez vérifier et configurer les paramètres de votre AWS Audit Manager à tout moment.

Pour accéder à vos paramètres

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.

Les paramètres suivants sont disponibles :

- Paramètres généraux
  - Autorisations
  - Chiffrement des données
  - Administrateur délégué (facultatif)
  - AWS Config (facultatif)
  - Security Hub (facultatif)
  - Désactiver AWS Audit Manager
- Paramètres d'évaluation
  - Propriétaires de l'audit par défaut (facultatif)
  - Destination du rapport d'évaluation (facultatif)
  - Notifications (facultatif)
- Paramètres de recherche de preuves
  - Outil de recherche de preuves (facultatif)
  - Destination de l'exportation (facultatif)

Paramètres généraux

L'onglet Paramètres généraux est l'affichage par défaut de la page des paramètres dans la console Audit Manager. Utilisez cet onglet pour vérifier et mettre à jour vos paramètres généraux d'Audit Manager.

Rubriques

- Autorisations
- Chiffrement des données
- Administrateur délégué (facultatif)
- AWS Config (facultatif)
- Security Hub (facultatif)
- Désactiver AWS Audit Manager

Autorisations

AWS Audit Manager utilise un rôle lié à un service pour se connecter aux sources de données en votre nom. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour AWS Audit Manager.

Pour consulter les détails du rôle lié au service utilisé par Audit Manager, choisissez Afficher l'autorisation du rôle lié au service IAM.

Pour plus d'informations sur l'utilisation des rôles liés à un service, consultez Utilisation des rôles liés à un service dans le Guide de l'utilisateur IAM.

Chiffrement des données

Audit Manager crée automatiquement un fichier unique Clé gérée par AWS pour le stockage sécurisé de vos données. Par défaut, vos données Audit Manager sont chiffrées avec cette clé KMS. Si vous souhaitez personnaliser les paramètres de chiffrement des données, vous pouvez également spécifier votre propre clé de chiffrement symétrique gérée par le client. L'utilisation de votre propre clé KMS vous donne plus de flexibilité dans la mesure où elle vous permet de créer, modifier ou désactiver des clés.

> **Important**
>
> Pour générer des rapports d'évaluation et exporter avec succès les résultats de recherche de preuves, votre clé gérée par le client (si vous en fournissez une) doit être identique à Région AWS que celle de votre évaluation. Pour obtenir la liste des régions d'Audit Manager, consultez AWS Audit Manager Points de terminaison et quotas dans Référence générale d'Amazon Web Services.

Vous pouvez mettre à jour vos paramètres de chiffrement des données à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

Audit Manager console

Pour mettre à jour vos paramètres de chiffrement des données (console)

1. Dans l'onglet Paramètres généraux, accédez à la section Chiffrement des données.
2. Pour utiliser la clé KMS par défaut fournie par Audit Manager, décochez la case Personnaliser les paramètres de chiffrement (avancés).
3. Pour utiliser une clé gérée par le client, sélectionnez la case Personnaliser les paramètres de chiffrement (avancé). Choisissez alors une clé KMS existante ou créez-en une.

AWS CLI

Pour mettre à jour vos paramètres de chiffrement des données (AWS CLI)

Exécutez la commande paramètres de mise à jour et utilisez le paramètre `--kms-key` pour préciser votre propre clé gérée par le client.

Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations.

```
aws auditmanager update-settings --kms-key arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Audit Manager API

Pour mettre à jour vos paramètres de chiffrement des données (API)

Appelez l'opération UpdateSettings et utilisez le paramètre kmSKey pour préciser votre propre clé gérée par le client.

Pour plus d'informations, choisissez les liens précédents dans le Guide de référence de l'API de l'Audit Manager. Il inclut des informations sur l'utilisation du fonctionnement et des paramètres dans l'un des SDK AWS spécifiques au langage.

> **Note**
>
> Lorsque vous modifiez vos paramètres de chiffrement des données d'Audit Manager, ces modifications s'appliquent à n'importe quelles nouvelles évaluations que vous créez. Cela inclut tous les rapports d'évaluation et les exportations de recherche de preuves que vous créez à partir de vos nouvelles évaluations.
>
> Les modifications ne s'appliquent pas aux évaluations existantes que vous avez créées avant de modifier vos paramètres de chiffrement. Cela inclut les nouveaux rapports d'évaluation et les exportations CSV que vous créez à partir d'évaluations existantes, en plus des rapports d'évaluation et des exportations CSV existants. Les évaluations existantes, ainsi que tous leurs rapports d'évaluation et exportations CSV, continuent d'utiliser l'ancienne clé KMS.
>
> Si l'identité IAM qui génère le rapport d'évaluation ne peut pas utiliser l'ancienne clé KMS, vous pouvez accorder des autorisations au niveau de la stratégie de clé. Pour obtenir des instructions, consultez Autoriser des utilisateurs d'autres comptes à utiliser une clé KMS dans le Guide du développeur d'AWS Key Management Service.

Pour toutes instructions sur la création de clés, consultez Création de clés dans le AWS Key Management Service Guide de l'utilisateur.

Administrateur délégué (facultatif)

Si vous utilisez AWS Organizations et souhaitez activer le support multi-comptes pour Audit Manager, vous pouvez désigner un compte membre de votre organisation en tant qu'administrateur délégué d'Audit Manager.

Prérequis

- Votre compte doit être membre d'une organisation. Pour plus d'informations, consultez la rubrique Création et gestion d'une organisation dans le Guide de l'utilisateur AWS Organizations.
- Avant de désigner un administrateur délégué, vous devez activer toutes les fonctionnalités de votre organisation. Vous devez également configurer les paramètres du Security Hub de votre organisation. Audit Manager peut ainsi collecter des preuves relatives au Security Hub à partir de vos comptes membres.
- Le compte d'administrateur délégué doit avoir accès à la clé KMS que vous avez fournie lors de la configuration d'Audit Manager. Pour consulter et modifier vos paramètres de chiffrement, consultez Chiffrement des données.

Considérations importantes pour les administrateurs délégués dans Audit Manager

Prenez note des facteurs suivants qui définissent le mode de fonctionnement de l'administrateur délégué dans Audit Manager :

Utilisation du compte de gestion

Vous ne pouvez pas utiliser votre compte de gestion AWS Organizations en tant qu'administrateur délégué dans Audit Manager.

Utilisation d'administrateurs délégués sur plusieurs Régions AWS

Si vous souhaitez activer Audit Manager dans plusieurs Région AWS, vous devez désigner un compte d'administrateur délégué séparément dans chaque région. Dans vos paramètres Audit Manager, vous devez désigner le même compte d'administrateur délégué dans toutes les régions.

Tâche de nettoyage de la recherche de preuves

Avant d'utiliser votre compte de gestion pour supprimer ou modifier un administrateur délégué, assurez-vous que le compte administrateur délégué actuel se connecte à Audit Manager et désactive l'outil de recherche de preuves. La désactivation de l'outil de recherche de preuves supprime automatiquement le magasin de données d'événements créé dans le compte lorsque l'outil de recherche de preuves a été activé.

Si cette tâche n'est pas terminée, le magasin de données d'événements reste dans leur compte. Dans ce cas, nous recommandons à l'administrateur délégué d'origine d'utiliser CloudTrail Lake pour supprimer manuellement le magasin de données d'événements.

Cette tâche de nettoyage est nécessaire pour éviter de vous retrouver avec plusieurs banques de données d'événements. Audit Manager ignore un magasin de données d'événements inutilisé une fois que vous avez supprimé ou modifié un compte d'administrateur délégué. Toutefois, si vous ne supprimez pas le magasin de données d'événements inutilisé, le magasin de données d'événements continue d'être soumis à des coûts de stockage liés à CloudTrail Lake.

Suppression de données

Lorsque vous supprimez un compte d'administrateur délégué pour Audit Manager, les données de ce compte ne sont pas supprimées. Si vous souhaitez supprimer les données de ressources d'un compte d'administrateur délégué, vous devez effectuer cette tâche séparément avant de supprimer le compte. Vous pouvez également réaliser cette opération dans la console Audit Manager. Vous pouvez également utiliser l'une des opérations d'API de suppression fournies

par Audit Manager. Pour obtenir la liste des opérations de suppression disponibles, consultez la section Suppression des données d'Audit Manager.

À l'heure actuelle, Audit Manager ne propose pas d'option permettant de supprimer des preuves pour un administrateur délégué spécifique. Au lieu de cela, lorsque votre compte de gestion annule l'enregistrement d'Audit Manager, nous procédons à un nettoyage du compte administrateur délégué actuel au moment de la désinscription.

Pour des solutions aux problèmes courants liés aux Organisations et aux administrateurs délégués dans Audit Manager, consultez Résolution des problèmes liés aux administrateurs délégués et à AWS Organizations.

Gestion de votre compte administrateur délégué pour Audit Manager

Vous pouvez consulter et modifier les paramètres de votre compte d'administrateur délégué comme suit.

Ajouter un administrateur délégué

Vous pouvez ajouter un administrateur délégué à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

> **Note**
>
> Une fois que vous avez ajouté un administrateur délégué dans vos paramètres d'Audit Manager, votre compte de gestion ne peut plus créer d'évaluations supplémentaires dans Audit Manager. En outre, la collecte de preuves s'arrête pour toutes les évaluations existantes créées par le compte de gestion. Audit Manager collecte et joint des preuves au compte de l'administrateur délégué, qui est le principal responsable de la gestion des évaluations de votre organisation.

Audit Manager console

Pour ajouter un administrateur délégué (console)

1. Dans l'onglet Paramètres généraux, accédez à la section Administrateur délégué.
2. Sous ID du compte d'administrateur délégué, entrez l'ID du compte de l'administrateur délégué.

3. Sélectionnez Déléguer.

AWS CLI

Pour ajouter un administrateur délégué (AWS CLI)

Exécutez la commande register-organization-admin-account et utilisez le `--admin-account-id` paramètre pour préciser l'ID du compte de l'administrateur délégué.

Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations.

```
aws auditmanager register-organization-admin-account --admin-account-id 111122223333
```

Audit Manager API

Pour ajouter un administrateur délégué (API)

Appelez l'opération RegisterOrganizationAdminAccount et utilisez le paramètre AdminAccountID pour préciser l'ID du compte de l'administrateur délégué.

Pour plus d'informations, choisissez les liens précédents dans le Guide de référence de l'API de l'Audit Manager. Il inclut des informations sur l'utilisation du fonctionnement et des paramètres dans l'un des SDK AWS spécifiques au langage.

Modifier un administrateur délégué

Vous pouvez modifier un administrateur délégué à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

> **Warning**
>
> Lorsque vous modifiez d'administrateur délégué, vous continuez à avoir accès aux preuves que vous avez précédemment collectées sous l'ancien compte d'administrateur délégué. Cependant, Audit Manager arrête de collecter et de joindre des preuves à l'ancien compte d'administrateur délégué.

Audit Manager console

Pour changer l'administrateur délégué actuel (console)

1. (Facultatif) Si l'administrateur délégué actuel (compte A) a activé l'outil de recherche de preuves, effectuez la tâche de nettoyage suivante :

   - Avant de désigner le compte B comme nouvel administrateur délégué, assurez-vous que le compte A se connecte à Audit Manager et désactive l'outil de recherche de preuves.

     La désactivation de l'outil de recherche de preuves supprime automatiquement le magasin de données d'événements créé lorsque le compte A a activé l'outil de recherche de preuves. Si vous n'effectuez pas cette étape, le compte A doit accéder à CloudTrail Lake et supprimer manuellement le magasin de données d'événements. Dans le cas contraire, le magasin de données d'événements reste dans le compte A et continue de faire l'objet de frais de stockage liés à CloudTrail Lake.
2. Dans l'onglet Paramètres généraux, accédez à la section Administrateur délégué et choisissez Supprimer.
3. Dans la fenêtre contextuelle qui s'affiche, choisissez Supprimer pour confirmer.
4. Sous ID du compte d'administrateur délégué, entrez l'ID du nouveau compte de l'administrateur délégué.
5. Sélectionnez Déléguer.

AWS CLI

Avant de commencer

Si l'administrateur délégué actuel (compte A) a activé l'outil de recherche de preuves, effectuez la tâche de nettoyage suivante :

Avant de désigner le compte B comme nouvel administrateur délégué, assurez-vous que le compte A se connecte à Audit Manager et désactive l'outil de recherche de preuves.

La désactivation de l'outil de recherche de preuves supprime automatiquement le magasin de données d'événements créé lorsque le compte A a activé l'outil de recherche de preuves. Si vous n'effectuez pas cette étape, le compte A doit accéder à CloudTrail Lake et supprimer manuellement le magasin de données d'événements. Dans le cas contraire, le magasin de données d'événements reste dans le compte A et continue de faire l'objet de frais de stockage liés à CloudTrail Lake.

Pour modifier l'administrateur délégué actuel (AWS CLI)

Commencez par exécuter la commande deregister-organization-admin-account à l'aide du paramètre `--admin-account-id` pour préciser l'ID du compte de l'administrateur délégué actuel.

Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Ensuite, exécutez la commande deregister-organization-admin-account à l'aide du paramètre `--admin-account-id` pour préciser l'ID du compte du nouvel administrateur délégué.

Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations.

```
aws auditmanager register-organization-admin-account --admin-account-id 444455556666
```

Audit Manager API

Avant de commencer

Si l'administrateur délégué actuel (compte A) a activé l'outil de recherche de preuves, effectuez la tâche de nettoyage suivante :

Avant de désigner le compte B comme nouvel administrateur délégué, assurez-vous que le compte A se connecte à Audit Manager et désactive l'outil de recherche de preuves.

La désactivation de l'outil de recherche de preuves supprime automatiquement le magasin de données d'événements créé lorsque le compte A a activé l'outil de recherche de preuves. Si vous n'effectuez pas cette étape, le compte A doit accéder à CloudTrail Lake et supprimer manuellement le magasin de données d'événements. Dans le cas contraire, le magasin de données d'événements reste dans le compte A et continue de faire l'objet de frais de stockage liés à CloudTrail Lake.

Pour modifier l'administrateur délégué (API) actuel

Appelez d'abord l'exécution deregister-organization-admin-account à l'aide du paramètre adminAccountId pour préciser l'ID du compte de l'administrateur délégué actuel.

Appelez ensuite l'opération RegisterOrganizationAdminAccount et utilisez le paramètre adminAccountID pour préciser l'ID du compte du nouvel administrateur délégué.

Pour plus d'informations, choisissez les liens précédents dans le Guide de référence de l'API de l'Audit Manager. Il inclut des informations sur l'utilisation du fonctionnement et des paramètres dans l'un des SDK AWS spécifiques au langage.

Supprimer un administrateur délégué

Vous pouvez supprimer un administrateur délégué à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

> **Warning**
>
> Lorsque vous supprimez un administrateur délégué, vous continuez à avoir accès aux preuves que vous avez précédemment collectées sous ce compte d'administrateur délégué. Cependant, Audit Manager arrête de collecter et de joindre des preuves à l'ancien compte d'administrateur délégué.

Audit Manager console

Pour supprimer l'administrateur délégué actuel (console)

1. (Facultatif) Si l'administrateur délégué actuel a activé l'outil de recherche de preuves, effectuez la tâche de nettoyage suivante :

   - Assurez-vous que le compte administrateur délégué actuel se connecte à Audit Manager et désactive l'outil de recherche de preuves.

     La désactivation de l'outil de recherche de preuves supprime automatiquement le magasin de données d'événements créé dans le compte lorsque l'outil de recherche de preuves a été activé. Si cette étape n'est pas terminée, le compte d'administrateur délégué doit utiliser CloudTrail Lake pour supprimer manuellement le magasin de données d'événements. Dans le cas contraire, le magasin de données d'événements reste dans le compte et continue de faire l'objet de frais de stockage liés à CloudTrail Lake.
2. Dans l'onglet Paramètres généraux, accédez à la section Administrateur délégué et choisissez Supprimer.

3. Dans la fenêtre contextuelle qui s'affiche, choisissez Supprimer pour confirmer.

AWS CLI

Avant de commencer

Si l'administrateur délégué actuel a activé l'outil de recherche de preuves, effectuez la tâche de nettoyage suivante :

Assurez-vous que le compte administrateur délégué actuel se connecte à Audit Manager et désactive l'outil de recherche de preuves.

La désactivation de l'outil de recherche de preuves supprime automatiquement le magasin de données d'événements créé dans le compte lorsque l'outil de recherche de preuves a été activé. Si cette étape n'est pas terminée, le compte d'administrateur délégué doit utiliser CloudTrail Lake pour supprimer manuellement le magasin de données d'événements. Dans le cas contraire, le magasin de données d'événements reste dans le compte et continue de faire l'objet de frais de stockage liés à CloudTrail Lake.

Pour supprimer l'administrateur délégué actuel (AWS CLI)

Exécutez la commande register-organization-admin-account et utilisez le paramètre `--admin-account-id` pour préciser l'ID du compte de l'administrateur délégué.

Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations.

```
aws auditmanager deregister-organization-admin-account --admin-account-
id 111122223333
```

Audit Manager API

Avant de commencer

Si l'administrateur délégué actuel a activé l'outil de recherche de preuves, effectuez la tâche de nettoyage suivante :

Assurez-vous que le compte administrateur délégué actuel se connecte à Audit Manager et désactive l'outil de recherche de preuves.

La désactivation de l'outil de recherche de preuves supprime automatiquement le magasin de données d'événements créé dans le compte lorsque l'outil de recherche de preuves a été activé. Si cette étape n'est pas terminée, le compte d'administrateur délégué doit utiliser CloudTrail Lake pour supprimer manuellement le magasin de données d'événements. Dans le cas contraire, le magasin de données d'événements reste dans le compte et continue de faire l'objet de frais de stockage liés à CloudTrail Lake.

Pour supprimer l'administrateur délégué (API) actuel

Appelez l'exécution deregister-organization-admin-account à l'aide du paramètre adminAccountId pour préciser l'ID du compte de l'administrateur délégué.

Pour plus d'informations, choisissez les liens précédents dans le Guide de référence de l'API de l'Audit Manager. Il inclut des informations sur l'utilisation du fonctionnement et des paramètres dans l'un des SDK AWS spécifiques au langage.

AWS Config (facultatif)

Vous pouvez autoriser Audit Manager à recueillir des résultats auprès de AWS Config. Lorsque AWS Config est activé, Audit Manager peut capturer des instantanés du niveau de sécurité de vos ressources en signalant les résultats des contrôles règlementaires directement depuis AWS Config. Nous vous recommandons vivement d'activer AWS Config pour une expérience optimale dans Audit Manager.

Pour activer AWS Config, choisissez Activer AWS Config pour accéder à ce service. Pour obtenir des instructions pour l'activation de AWS Config, consultez Configuration AWS Config dans le AWS Config Guide du développeur.

Security Hub (facultatif)

Vous pouvez autoriser Audit Manager à importer les résultats AWS Security Hub correspondant à toutes les normes de conformité prises en charge. Lorsque Security Hub est activé, Audit Manager peut capturer des instantanés du niveau de sécurité de vos ressources en signalant les résultats des contrôles de sécurité directement depuis Security Hub. Nous vous recommandons vivement d'activer Security Hub pour une expérience optimale dans Audit Manager.

Pour activer Security Hub, choisissez Enable Security Hub pour accéder à ce service. Pour toutes instructions sur la façon d'activer Security Hub, veuillez consulter Configuration AWS Security Hub dans le Guide de l'utilisateur de Security Hub.

Désactiver AWS Audit Manager

Vous pouvez désactiver Audit Manager si vous ne souhaitez plus utiliser le service. Lorsque vous désactivez Audit Manager, vous avez également la possibilité de supprimer toutes vos données.

Par défaut, vos données ne sont pas supprimées lorsque vous désactivez Audit Manager. Vos données de preuve sont conservées pendant deux ans à compter de leur création. Vos autres ressources d'Audit Manager (y compris les évaluations, les contrôles personnalisés et les frameworks personnalisés) sont conservées indéfiniment et seront disponibles si vous réactivez Audit Manager ultérieurement. Pour plus d'informations sur la conservation des données, veuillez consulter Protection des données dans ce guide.

Si vous choisissez de supprimer vos données, Audit Manager supprime toutes les données probantes ainsi que toutes les ressources d'Audit Manager que vous avez créées (y compris les évaluations, les contrôles personnalisés et les frameworks personnalisés). Toutes vos données sont supprimées dans les sept jours suivant la désactivation d'Audit Manager.

⚠ Warning

- Lorsque vous désactivez Audit Manager, votre accès est révoqué et le service ne collecte plus de preuves pour les évaluations existantes. Vous ne pouvez accéder à aucun élément du service à moins de réactiver Audit Manager.
- La suppression de toutes les données est une action permanente. Si vous décidez de réactiver Audit Manager ultérieurement, vos données ne seront pas récupérables.

Vous pouvez désactiver Audit Manager à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

Audit Manager console

Pour désactiver Audit Manager (console)

1. Dans l'onglet Paramètres généraux, accédez à la section Désactiver AWS Audit Manager.
2. Choisissez Désactiver.
3. Dans la fenêtre contextuelle, vérifiez votre paramètre actuel de conservation des données.
   a. Pour poursuivre votre sélection actuelle, choisissez Désactiver Audit Manager.

b. Pour modifier votre sélection actuelle, effectuez les étapes suivantes :

   i. Choisissez Annuler pour revenir à la page des paramètres.

   ii. Pour utiliser le paramètre de conservation des données par défaut, désactivez Supprimer toutes les données. Cette sélection conserve les données probantes pendant deux ans à compter de sa création, et conserve indéfiniment les autres ressources de l'Audit Manager.

   iii. Pour supprimer vos données, activez Supprimer toutes les données.

   iv. Choisissez Désactiver, puis Désactiver Audit Manager pour confirmer votre choix.

AWS CLI

Avant de commencer

Avant de désactiver Audit Manager, vous pouvez exécuter la commande update-settings pour définir votre politique de conservation des données préférée. Par défaut, Audit Manager conserve vos données. Si vous souhaitez demander la suppression de vos données, utilisez le paramètre `--deregistration-policy` dont la valeur `deleteResources` est définie sur `ALL`.

```
aws auditmanager update-settings --deregistration-policy deleteResources=ALL
```

Pour désactiver Audit Manager (AWS CLI)

Lorsque vous êtes prêt à désactiver Audit Manager, exécutez la commande deregister-account.

```
aws auditmanager deregister-account
```

Audit Manager API

Avant de commencer

Avant de désactiver Audit Manager, vous pouvez utiliser l'opération d'API UpdateSettings pour définir votre politique de conservation des données préférée. Par défaut, Audit Manager conserve vos données. Si vous souhaitez supprimer vos données, vous pouvez utiliser l'attribut DeRegistrationPolicy pour demander la suppression de vos données.

Pour désactiver Audit Manager (API)

Lorsque vous êtes prêt à désactiver Audit Manager, appelez l'opération DeRegisterAccount.

Pour plus d'informations, choisissez les liens précédents dans le Guide de référence de l'API de l'Audit Manager. Il inclut des informations sur l'utilisation du fonctionnement et des paramètres dans l'un des SDK AWS spécifiques au langage.

Pour réactiver Audit Manager après l'avoir désactivé

Accédez à la page d'accueil du service Audit Manager et suivez les étapes pour configurer Audit Manager en tant que nouvel utilisateur. Pour de plus amples informations, veuillez consulter Configuration de AWS Audit Manager.

> **Tip**
>
> - Si vous avez choisi de supprimer vos données lorsque vous avez désactivé Audit Manager, vous devez attendre qu'elles soient supprimées avant de pouvoir réactiver le service. Selon la quantité de données dont vous disposez, cela peut prendre jusqu'à sept jours. Cependant, n'hésitez pas à essayer de réactiver Audit Manager avant cette date. Dans de nombreux cas, les données sont supprimées en une heure seulement.
> - Si vous choisissez de ne pas supprimer vos données lorsque vous désactivez Audit Manager, vos évaluations existantes passent à l'état inactif et cessent de collecter des preuves. Pour qu'une évaluation préexistante recommence à collecter des preuves, modifiez l'évaluation et choisissez Enregistrer sans apporter de modifications.

Paramètres d'évaluation

Utilisez cet onglet pour revoir et mettre à jour vos paramètres d'évaluation.

Rubriques

- Propriétaires de l'audit par défaut (facultatif)
- Destination du rapport d'évaluation (facultatif)
- Notifications (facultatif)

Propriétaires de l'audit par défaut (facultatif)

Vous pouvez spécifier les propriétaires d'audit par défaut qui ont un accès principal à vos évaluations dans Audit Manager.

Vous pouvez mettre à jour ce paramètre à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

Audit Manager console

Vous pouvez choisir parmi les options Comptes AWS répertoriées dans le tableau ou utiliser la barre de recherche pour en rechercher d'autres Comptes AWS.

Pour mettre à jour les paramètres de vos responsables d'audit par défaut (console)

1. Dans l'onglet Paramètres d'évaluation, accédez à la section Responsables d'audit par défaut et choisissez Modifier.
2. Pour ajouter un responsable d'audit par défaut, sélectionnez la case à cocher en regard du nom du compte sous Responsable de l'audit.
3. Pour supprimer un responsable d'audit par défaut, videz la case à cocher en regard du nom du compte sous Responsable de l'audit.
4. Lorsque vous avez terminé, sélectionnez Enregistrer.

AWS CLI

Pour mettre à jour les paramètres de vos responsables d'audit par défaut (AWS CLI)

Exécutez la commande paramètres de mise à jour et utilisez le paramètre `--default-process-owners` pour préciser un responsable d'audit.

Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations. Notez que `roleType` ne peut être que `PROCESS_OWNER`.

```
aws auditmanager update-settings --default-process-owners
 roleType=PROCESS_OWNER,roleArn=arn:aws:iam::111122223333:role/Administrator
```

Audit Manager API

Pour mettre à jour les paramètres de vos responsables d'audit par défaut (API)

Appelez l'opération UpdateSettings et utilisez le paramètre DefaultProcessOwners pour préciser les responsables d'audit par défaut. Notez que `roleType` ne peut être que `PROCESS_OWNER`.

Pour plus d'informations sur les responsables d'audit, consultez Responsables d'audit dans la section Concepts et terminologie de ce guide.

Destination du rapport d'évaluation (facultatif)

Lorsque vous générez un rapport d'évaluation, Audit Manager publie le rapport dans le compartiment S3 de votre choix. Ce compartiment S3 est appelé destination du rapport d'évaluation. Vous pouvez choisir le compartiment Amazon S3 dans lequel Audit Manager stocke vos rapports d'évaluation.

Vous pouvez mettre à jour ce paramètre à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

Audit Manager console

Pour mettre à jour les paramètres de destination de votre rapport d'évaluation (console)

1. Dans l'onglet Paramètres d'évaluation, accédez à la section Destination du rapport d'évaluation.
2. Pour utiliser un compartiment Amazon S3 existant, sélectionnez un nom de compartiment dans le menu déroulant.
3. Pour créer un nouveau compartiment Amazon S3, choisissez Créer un nouveau compartiment.
4. Lorsque vous avez terminé, sélectionnez Enregistrer.

AWS CLI

Pour mettre à jour les paramètres de destination de votre rapport d'évaluation (AWS CLI)

Exécutez la commande paramètres de mise à jour et utilisez le paramètre `--default-assessment-reports-destination` pour préciser un compartiment S3.

Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations :

```
aws auditmanager update-settings --default-assessment-reports-destination
 destinationType=S3,destination=s3://doc-example-destination-bucket
```

Audit Manager API

Pour mettre à jour les paramètres de destination de votre rapport d'évaluation (API)

Appelez l'opération UpdateSettings et utilisez le paramètre DefaultProcessOwners pour préciser un compartiment S3.

Pour plus d'informations sur la façon de créer un compartiment S3, consultez Création d'un compartiment dans le Guide de l'utilisateur Amazon S3.

Conseils de configuration pour la destination de votre rapport d'évaluation

Pour garantir la bonne génération de votre rapport d'évaluation, nous vous recommandons de vérifier les configurations suivantes pour la destination de votre rapport d'évaluation.

Compartiments de la même région

Nous vous recommandons d'utiliser un compartiment S3 qui se trouve dans le même compartiment Région AWS que votre évaluation. Lorsque vous utilisez un compartiment et une évaluation correspondant à la même région, votre rapport d'évaluation peut inclure jusqu'à 22 000 éléments de preuve. À l'inverse, lorsque vous utilisez un compartiment et une évaluation interrégionaux, seuls 3 500 éléments de preuve peuvent être inclus.

Région AWS

La Région AWS de la clé gérée par votre client (si vous en avez fourni une) doit correspondre à la région de votre évaluation et au compartiment S3 de destination de votre rapport d'évaluation. Pour obtenir des instructions sur la modification de la clé KMS, consultez AWS Audit Manager Paramètres, Chiffrement des données. Pour obtenir des instructions sur la modification du compartiment S3, consultez AWS Audit Manager Paramètres, Destination du rapport d'évaluation. Pour obtenir la liste des régions d'Audit Manager, consultez AWS Audit Manager Points de terminaison et quotas dans Référence générale d'Amazon Web Services.

Chiffrement de compartiment S3

Si la destination de votre rapport d'évaluation dispose d'une politique de compartiment qui nécessite un chiffrement côté serveur (SSE) à l'aide de SSE-KMS, la clé KMS utilisée dans cette politique de compartiment doit correspondre à la clé KMS que vous avez configurée dans les paramètres de chiffrement des données d'Audit Manager. Si vous n'avez pas configuré de clé KMS dans vos paramètres d'Audit Manager et que votre politique de compartiment de destination du rapport d'évaluation nécessite SSE, assurez-vous que la politique de compartiment autorise SSE-S3. Pour obtenir des instructions sur la configuration de la clé KMS utilisée pour le chiffrement des données, consultez la section Paramètres de chiffrement des données.

Compartiments S3 entre comptes

L'utilisation d'un compartiment S3 multi-comptes comme destination de votre rapport d'évaluation n'est pas prise en charge dans la console Audit Manager. Il est possible de spécifier un compartiment multi-comptes comme destination de votre rapport d'évaluation en utilisant le AWS CLI ou l'un des SDK AWS, mais pour des raisons de simplicité, nous vous recommandons de ne pas le faire. Si vous choisissez d'utiliser un compartiment S3 multi-comptes comme destination de votre rapport d'évaluation, tenez compte des points suivants.

- Par défaut, les objets S3, tels que les rapports d'évaluation, appartiennent à Compte AWS celui qui télécharge l'objet. Vous pouvez utiliser le paramètre propriété de l'objet S3 pour modifier ce comportement par défaut afin que tous les nouveaux objets écrits par des comptes avec la liste de contrôle d'accès (ACL) `bucket-owner-full-control` prédéfinie deviennent automatiquement la propriété du propriétaire du compartiment (ACL) prédéfinie.

  Bien que cela ne soit pas obligatoire, nous vous recommandons d'apporter les modifications suivantes aux paramètres de votre compartiment multi-comptes. Ces modifications garantissent que le propriétaire du compartiment a le contrôle total des rapports d'évaluation que vous publiez dans son compartiment.

  - Définissez la propriété de l'objet du compartiment S3 selon les préférences du propriétaire du compartiment, au lieu du rédacteur d'objets par défaut
  - Ajoutez une politique de compartiment pour garantir que les objets chargés dans ce compartiment disposent de l'ACL `bucket-owner-full-control`
- Pour permettre à Audit Manager de publier des rapports dans un compartiment S3 multi-comptes, vous devez ajouter la politique de compartiment S3 suivante à la destination de votre rapport d'évaluation. Remplacez chaque *`espace réservé`* par vos propres informations. L'élément `Principal` de cette politique est l'utilisateur ou le rôle qui possède l'évaluation et crée le rapport d'évaluation. Le `Resource` précise le compartiment S3 entre comptes dans lequel le rapport est publié.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account assessment report publishing",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
```

```
            },
            "Action": [
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:PutObjectAcl",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
            ]
        }
    ]
}
```

Notifications (facultatif)

Audit Manager peut envoyer des notifications à la rubrique Amazon SNS que vous spécifiez dans ce paramètre. Si vous êtes abonné à cette rubrique SNS, vous recevez des notifications lorsque vous vous connectez à Audit Manager.

Vous pouvez mettre à jour ce paramètre à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

Audit Manager console

Pour mettre à jour vos paramètres de notification (console)

1. Dans l'onglet Paramètres d'évaluation, accédez à la section Notifications.
2. Pour utiliser une rubrique SNS existante, sélectionnez son nom dans le menu déroulant.
3. Pour créer une nouvelle rubrique SNS, choisissez Créer une nouvelle rubrique.
4. Lorsque vous avez terminé, sélectionnez Enregistrer.

AWS CLI

Pour mettre à jour vos paramètres de notification (AWS CLI)

Exécutez la commande paramètres de mise à jour et utilisez le paramètre `--sns-topic` pour préciser une rubrique SNS.

Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations :

```
aws auditmanager update-settings --sns-topic arn:aws:sns:us-east-1:111122223333:my-assessment-topic
```

Audit Manager API

Pour mettre à jour vos paramètres de notification (API)

Appelez l'opération UpdateSettings et utilisez le paramètre SNSTopic pour spécifier une rubrique SNS.

> **Note**
>
> Vous pouvez utiliser une rubrique SNS standard ou une rubrique SNS FIFO (premier entré, premier sorti). Bien qu'Audit Manager prenne en charge l'envoi de notifications aux rubriques FIFO, l'ordre dans lequel les messages sont envoyés n'est pas garanti.
> Si vous voulez utiliser une rubrique Amazon SNS qui ne vous appartient pas, configurez votre politique (IAM) AWS Identity and Access Management pour cela. Plus précisément, vous devez la configurer pour autoriser la publication de la rubrique à partir de l'Amazon Resource Name (ARN). Pour de plus amples informations sur IAM, consultez Gestion d'accès et identité pour AWS Audit Manager.

Pour en savoir plus sur la liste des actions qui invoquent des notifications dans Audit Manager, consultezNotifications dans AWS Audit Manager.

Pour obtenir des instructions sur la création d'une rubrique Amazon SNS, consultez la section Création d'une rubrique Amazon SNS dans le guide de l'utilisateur Amazon SNS.

Paramètres de recherche de preuves

Utilisez cet onglet pour revoir et mettre à jour vos paramètres de l'outil de recherche de preuves.

Rubriques

- Outil de recherche de preuves (facultatif)
- Destination de l'exportation (facultatif)

Outil de recherche de preuves (facultatif)

Nous vous recommandons vivement d'activer l'outil de recherche de preuves. L'activation de cette fonctionnalité est nécessaire si vous souhaitez exécuter des requêtes de recherche sur vos preuves.

Suivez ces étapes pour activer, désactiver ou vérifier l'état de l'outil de recherche de preuves.

Activer l'outil de recherche d'éléments probants

Vous devez activer l'outil de recherche de preuves dans chaque Région AWS endroit où vous souhaitez rechercher des preuves. Si vous êtes un administrateur délégué pour Audit Manager, activez l'outil de recherche de preuves pour rechercher des preuves pour tous les comptes membres de votre organisation.

Autorisations requises pour activer l'outil de recherche de preuves

Pour activer l'outil de recherche de preuves, vous devez disposer d'autorisations pour créer et gérer un magasin de données d'événement dans CloudTrail Lake. Pour utiliser cette fonctionnalité, vous devez disposer des autorisations nécessaires pour effectuer des requêtes CloudTrail Lake. Pour un exemple de politique d'autorisation que vous pouvez utiliser, voir Autoriser un accès administrateur complet.

Si vous avez besoin d'aide concernant les autorisations, contactez votre administrateur AWS. Si vous êtes un administrateur AWS, vous pouvez copier la déclaration d'autorisation requise et la joindre à une politique IAM.

Demande d'activation de l'outil de recherche de preuves

Vous pouvez terminer cette tâche à l'aide de la console Audit Manager, le AWS Command Line Interface (AWS CLI) ou l'API Audit Manager.

Audit Manager console

Pour demander l'activation de l'outil de recherche de preuves (console)

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.

2. Dans l'onglet Paramètres de l'outil de recherche de preuves, accédez à la section Recherche de preuves.
3. Choisissez Politique d'autorisation requise, puis Afficher les autorisations CloudTrail Lake pour consulter les autorisations requises pour l'outil de recherche de preuves. Si vous ne disposez pas encore de ces autorisations, vous pouvez copier cette déclaration de politique et la joindre à une politique IAM.
4. Sélectionnez Activer.
5. Dans la fenêtre contextuelle, choisissez Request to enable.

AWS CLI

Pour demander l'activation de l'outil de recherche de preuves (AWS CLI)

Exécutez la commande update-settings avec le paramètre `--evidence-finder-enabled`.

```
aws auditmanager update-settings --evidence-finder-enabled
```

Audit Manager API

Pour demander l'activation de l'outil de recherche de preuves (API)

Appelez l'opération UpdateSettings et utilisez le paramètre evidenceFinderEnabled.

Pour plus d'informations, choisissez les liens précédents dans le Guide de référence de l'API de l'Audit Manager. Il inclut des informations sur l'utilisation du fonctionnement et des paramètres dans l'un des SDK AWS spécifiques au langage.

Confirmer le statut de l'outil de recherche de preuves

Après avoir soumis votre demande, il faut jusqu'à 10 minutes pour activer l'outil de recherche de preuves et créer un magasin de données sur les événements. Dès que le magasin de données d'événements est créé, toutes les nouvelles preuves sont ensuite ingérées dans le magasin de données d'événements.

Lorsque l'outil de recherche de preuves est activé et que le magasin de données sur les événements est créé, nous remplissons le nouveau magasin de données sur les événements avec un maximum de deux ans de vos preuves passées. Ce processus se déroule automatiquement et prend jusqu'à sept jours.

Vous pouvez vérifier l'état actuel de l'outil de recherche de preuves à l'aide de la console Audit Manager, de AWS CLI ou de l'API Audit Manager.

Audit Manager console

Pour afficher l'état actuel de l'outil de recherche de preuves (console)

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Sous Activer l'outil de recherche de preuves (facultatif), consultez l'état actuel.

   Chaque état est défini comme suit :

   - L'outil de recherche de preuves n'est pas activé : vous n'avez pas encore activé l'outil de recherche de preuves avec succès.
   - Vous avez demandé d'activer l'outil de recherche de preuves. Votre demande est en attente de la création du magasin de données sur les événements.
   - L'outil de recherche de preuves est activé : le magasin de données sur les événements a été créé. Vous pouvez désormais utiliser l'outil de recherche de preuves.

     En fonction de la quantité de preuves dont vous disposez, il faut jusqu'à sept jours pour remplir le nouveau magasin de données d'événements avec vos données de preuves antérieures. Un panneau d'information bleu indique que le remplissage des données est en cours. Entre-temps, n'hésitez pas à commencer à explorer l'outil de recherche de preuves. Cependant, n'oubliez pas que toutes les données ne sont pas disponibles tant que le remblayage n'est pas terminé.
   - Vous avez demandé à désactiver l'outil de recherche de preuves : votre demande est en attente de la suppression du magasin de données sur les événements.
   - L'outil de recherche de preuves a été désactivé : l'outil de recherche de preuves a été définitivement désactivé et le magasin de données d'événements est supprimé.

AWS CLI

Pour afficher l'état actuel de l'outil de recherche de preuves (AWS CLI)

Exécutez la commande update-settings avec le paramètre `--attribute`défini sur `EVIDENCE_FINDER_ENABLEMENT`.

```
aws auditmanager get-settings --attribute EVIDENCE_FINDER_ENABLEMENT
```

Cela renvoie les informations suivantes :

enablementStatus

Cet attribut indique l'état actuel de l'outil de recherche de preuves.

- `ENABLE_IN_PROGRESS` : vous avez demandé d'activer l'outil de recherche de preuves. Un magasin de données sur les événements est en cours de création pour répondre aux requêtes de recherche de preuves.
- `ENABLED` : un magasin de données sur les événements a été créé et l'outil de recherche de preuves est activé. Nous vous recommandons d'attendre sept jours jusqu'à ce que le magasin de données sur les événements soit rempli avec vos anciennes données probantes. Vous pouvez utiliser l'outil de recherche de preuves en attendant, mais toutes les données ne sont pas disponibles tant que le remplissage n'est pas terminé.
- `DISABLE_IN_PROGRESS` : vous avez demandé à désactiver l'outil de recherche de preuves, et votre demande est en attente de suppression de la banque de données des événements.
- `DISABLED` : vous avez définitivement désactivé l'outil de recherche de preuves et le magasin de données de l'événement est supprimé. Vous ne pouvez pas réactiver l'outil de recherche de preuves après ce point.

backfillStatus

Cet attribut indique l'état actuel du remplissage des données de preuve.

- `NOT_STARTED` : le remplissage n'a pas encore commencé.
- `IN_PROGRESS` : le remplissage est en cours. Cela prend jusqu'à sept jours, selon la quantité de données de preuve.
- `COMPLETED` : le remblayage est terminé. Toutes vos preuves passées sont désormais interrogeables.

Audit Manager API

Pour afficher l'état actuel de l'outil de recherche de preuves (API)

Appelez l'opération GetSettings avec le paramètre `attribute` défini sur `EVIDENCE_FINDER_ENABLEMENT`. Cela renvoie les informations suivantes :

enablementStatus

Cet attribut indique l'état actuel de l'outil de recherche de preuves.

- `ENABLE_IN_PROGRESS` : vous avez demandé d'activer l'outil de recherche de preuves. Un magasin de données sur les événements est en cours de création pour répondre aux requêtes de recherche de preuves.
- `ENABLED` : un magasin de données sur les événements a été créé et l'outil de recherche de preuves est activé. Nous vous recommandons d'attendre sept jours jusqu'à ce que le magasin de données sur les événements soit rempli avec vos anciennes données probantes. Vous pouvez utiliser l'outil de recherche de preuves en attendant, mais toutes les données ne sont pas disponibles tant que le remplissage n'est pas terminé.
- `DISABLE_IN_PROGRESS` : vous avez demandé à désactiver l'outil de recherche de preuves, et votre demande est en attente de suppression de la banque de données des événements.
- `DISABLED` : vous avez définitivement désactivé l'outil de recherche de preuves et le magasin de données de l'événement est supprimé. Vous ne pouvez pas réactiver l'outil de recherche de preuves après ce point.

backfillStatus

Cet attribut indique l'état actuel du remplissage des données de preuve.

- `NOT_STARTED` signifie que le remplissage n'a pas encore commencé.
- `IN_PROGRESS` signifie que le remplissage est en cours. Cela prend jusqu'à sept jours, selon la quantité de données de preuve.
- `COMPLETED` signifie que le remplissage est terminé. Toutes vos preuves passées sont désormais interrogeables.

Pour plus d'informations, consultez evidenceFinderEnablement dans le manuel de référence de l'API Audit Manager.

Désactiver l'outil de recherche d'éléments probants

Si vous ne souhaitez plus utiliser l'outil de recherche de preuves, vous pouvez désactiver cette fonctionnalité à tout moment.

> **Warning**
>
> La désactivation de l'outil de recherche de preuves supprime le magasin de données d'événements CloudTrail Lake créé par Audit Manager. Par conséquent, vous ne pouvez pas réactiver cette fonctionnalité. Pour réutiliser l'outil de recherche de preuve après l'avoir désactivé, vous devez désactiver AWS Audit Manager puis réactiver complètement le service.

Autorisations requises pour désactiver l'outil de recherche de preuve

Pour désactiver l'outil de recherche de preuve, vous devez disposer d'autorisations pour supprimer un magasin de données d'événement dans CloudTrail Lake. Pour un exemple de politique que vous pouvez utiliser, consultez Autorisations pour désactiver l'outil de recherche de preuves.

Si vous avez besoin d'aide concernant les autorisations, contactez votre administrateur AWS. Si vous êtes un administrateur AWS, vous pouvez joindre la déclaration d'autorisation requise à une politique IAM.

Désactivation de l'outil de recherche de preuves

Vous pouvez terminer cette tâche à l'aide de la console Audit Manager, le AWS Command Line Interface (AWS CLI) ou l'API Audit Manager.

Audit Manager console

Pour désactiver l'outil de recherche de preuves (console)

1. Dans la section Outil de recherche de preuves de la page des paramètres d'Audit Manager, choisissez Désactiver.
2. Dans la fenêtre contextuelle qui apparaît, entrez **`Yes`** pour confirmer votre décision.
3. Choisissez Demande pour désactiver.

AWS CLI

Pour désactiver l'outil de recherche de preuves (AWS CLI)

Exécutez la commande update-settings avec le paramètre `--no-evidence-finder-enabled`.

```
aws auditmanager update-settings --no-evidence-finder-enabled
```

Audit Manager API

Pour désactiver l'outil de recherche de preuves (API)

Appelez l'opération UpdateSettings et utilisez le paramètre evidenceFinderEnabled.

Pour plus d'informations, choisissez les liens précédents dans le Guide de référence de l'API de l'Audit Manager. Il inclut des informations sur l'utilisation du fonctionnement et des paramètres dans l'un des SDK AWS spécifiques au langage.

Destination de l'exportation (facultatif)

Lorsque vous exécutez des requêtes dans l'outil de recherche de preuves, vous pouvez exporter les résultats de vos recherches dans un fichier de valeurs séparées par des virgules (CSV). Utilisez ce paramètre pour choisir le compartiment S3 par défaut dans lequel Audit Manager enregistre vos fichiers exportés.

Vous pouvez mettre à jour ce paramètre à l'aide de la console Audit Manager, du AWS Command Line Interface (AWS CLI) ou de l'API Audit Manager.

> **Important**
>
> Votre compartiment S3 doit disposer de la politique d'autorisation requise pour permettre à CloudTrail d'y écrire les fichiers d'exportation. Plus précisément, la politique de compartiment doit inclure une action `s3:PutObject` et l'ARN du compartiment, et répertorier CloudTrail comme principal de service. Nous fournissons un exemple de politique d'autorisation que vous pouvez utiliser. Pour savoir comment joindre cette politique à votre compartiment S3, consultez Ajout d'une stratégie de compartiment à l'aide de la console Amazon S3.
> Pour plus de conseils, consultez les conseils de configuration pour votre destination d'exportation sur cette page.

Audit Manager console

Pour mettre à jour vos paramètres de destination d'exportation (console)

1. Dans l'onglet Paramètres de l'outil de recherche de preuves, accédez à la section Destination d'exportation.
2. Choisissez l'une des options suivantes :
   - Si vous souhaitez supprimer le compartiment S3 actuel, choisissez Supprimer pour effacer vos paramètres.
   - Si vous souhaitez enregistrer un compartiment S3 par défaut pour la première fois, passez à l'étape 3.
3. Précisez le compartiment S3 dans lequel vous souhaitez stocker vos fichiers exportés.
   - Choisissez Navigateur S3 pour faire votre choix dans la liste de vos compartiments.
   - Vous pouvez également saisir l'URI du compartiment au format suivant : **`s3://bucketname/prefix`**

   > **Tip**
   >
   > Pour que votre compartiment de destination reste organisé, vous pouvez créer un dossier facultatif pour vos exportations CSV. Pour ce faire, ajoutez une barre oblique (**`/`**) et un préfixe à la valeur dans la zone URI de ressource (par exemple, **`/evidenceFinderCSVExports`**). Audit Manager ajoutera alors ce préfixe lors de l'envoi du fichier CSV au compartiment et Amazon S3 génèrera le chemin spécifié par le préfixe. Pour plus d'informations sur les préfixes dans Amazon S3, veuillez consulter Organisation des objets dans la console Amazon S3 dans le Guide de l'utilisateur Amazon Simple Storage Service.
4. Lorsque vous avez terminé, sélectionnez Enregistrer.

Pour plus d'informations sur la façon de créer un compartiment S3, consultez Création d'un compartiment dans le Guide de l'utilisateur Amazon S3.

AWS CLI

Pour mettre à jour vos paramètres de destination d'exportation (AWS CLI)

Exécutez la commande paramètres de mise à jour et utilisez le paramètre `--default-export-destination` pour préciser un compartiment S3.

Dans l'exemple suivant, remplacez *le texte de l'espace réservé* par vos propres informations :

```
aws auditmanager update-settings --default-export-destination
 destinationType=S3,destination=s3://doc-example-destination-bucket
```

Pour obtenir des instructions sur la création d'un compartiment S3, consultez la section create-bucket dans le manuel AWS CLI Référence de commandes.

Audit Manager API

Pour mettre à jour vos paramètres de destination d'exportation (API)

Appelez l'opération UpdateSettings et utilisez le paramètre defaultExportDestination pour préciser un compartiment S3.

Pour obtenir des instructions sur la création d'un compartiment S3, consultez la section create-bucket dans le Amazon S3 API Reference.

Conseils de configuration pour votre destination d'exportation

Pour garantir une exportation de fichiers réussie, nous vous recommandons de vérifier les configurations suivantes pour votre destination d'exportation.

Région AWS

La Région AWS de la clé gérée par votre client (si vous en avez fourni une) doit correspondre à la région de votre évaluation. Pour obtenir des instructions sur la modification de la clé KMS, consultez Paramètres du chiffrement des données Audit Manager.

Compartiments S3 entre comptes

L'utilisation d'un compartiment S3 multi-comptes comme destination de votre rapport n'est pas prise en charge dans la console Audit Manager. Il est possible de spécifier un compartiment multi-comptes en utilisant le AWS CLI ou l'un des SDK AWS, mais pour des raisons de simplicité, nous vous recommandons de ne pas le faire. Si vous choisissez d'utiliser un compartiment S3 multi-comptes comme destination de votre export, tenez compte des points suivants.

- Par défaut, les objets S3, tels que les exportations CSV, appartiennent à Compte AWS celui qui télécharge l'objet. Vous pouvez utiliser le paramètre propriété de l'objet S3 pour modifier ce comportement par défaut afin que tous les nouveaux objets écrits par des comptes avec la liste de contrôle d'accès (ACL) `bucket-owner-full-control` prédéfinie deviennent automatiquement la propriété du propriétaire du compartiment (ACL) prédéfinie.

  Bien que cela ne soit pas obligatoire, nous vous recommandons d'apporter les modifications suivantes aux paramètres de votre compartiment multi-comptes. Ces modifications garantissent que le propriétaire du compartiment a le contrôle total des fichiers exportés que vous publiez dans son compartiment.

  - Définissez la propriété de l'objet du compartiment S3 selon les préférences du propriétaire du compartiment, au lieu du rédacteur d'objets par défaut
  - Ajoutez une politique de compartiment pour garantir que les objets chargés dans ce compartiment disposent de l'ACL `bucket-owner-full-control`

- Pour permettre à Audit Manager de publier des rapports dans un compartiment S3 multi-comptes, vous devez ajouter la politique de compartiment S3 suivante au compartiment de destination d'exportation de votre rapport d'évaluation. Remplacez chaque *`espace réservé`* par vos propres informations. L'élément `Principal` de cette politique est l'utilisateur ou le rôle qui possède l'évaluation et exporte le fichier. Le `Resource` précise le compartiment S3 entre comptes dans lequel le fichier est exporté.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "Allow cross account file exports",
          "Effect": "Allow",
          "Principal": {
              "AWS":
 "arn:aws:iam::AssessmentOwnerAccountId:user/AssessmentOwnerUserName"
          },
          "Action": [
              "s3:ListBucket",
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetBucketLocation",
              "s3:PutObjectAcl",
              "s3:DeleteObject"
          ],
```

```
            "Resource": [
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET",
                "arn:aws:s3:::CROSS-ACCOUNT-BUCKET/*"
            ]
        }
    ]
}
```

Notifications dans AWS Audit Manager

AWS Audit Manager peut vous informer des actions des utilisateurs par le biais d'Amazon Simple Notification Service (Amazon SNS).

Audit Manager envoie des notifications quand l'un des événements suivants se produit :

- Le propriétaire de l'audit délègue un ensemble de contrôles à des fins de révision.
- Un délégué soumet un ensemble de contrôles révisé au propriétaire de l'audit.
- Le propriétaire de l'audit effectue la révision d'un ensemble de contrôles.

Prérequis

Avant de configurer des notifications Amazon SNS dans Audit Manager, assurez-vous d'effectuer les étapes suivantes.

1. Créez une rubrique dans Amazon SNS si vous n'en avez pas. Des instructions sont disponibles dans la section Création d'une rubrique Amazon SNS du Manuel du développeur Amazon Simple Notification Service.
2. Abonnez au moins un point de terminaison pour la rubrique. Par exemple, si vous voulez recevoir des notifications par SMS, abonnez un point de terminaison SMS à la rubrique. Un point de terminaison SMS est un numéro de téléphone portable. Pour recevoir des notifications par e-mail, abonnez un point de terminaison de messagerie à la rubrique. Un point de terminaison de messagerie est une adresse e-mail.

   Pour en savoir plus, consultez Mise en route dans le Guide du développeur Amazon Simple Notification Service.
3. (Facultatif) Si votre rubrique utilise AWS Key Management Service (AWS KMS) pour le chiffrement côté serveur (SSE), vous devez ajouter des autorisations à la stratégie AWS KMS key. Pour obtenir un exemple de stratégie à utiliser, consultez Autorisations pour une clé KMS attachée à une rubrique SNS.

Configuration des notifications dans AWS Audit Manager

Procédez comme suit pour configurer vos notifications dans AWS Audit Manager.

Pour configurer les notifications dans AWS Audit Manager

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Sous Notifications - facultatif, précisez la rubrique SNS à utiliser pour recevoir des notifications.
   - Pour utiliser une rubrique existante, sélectionnez son nom dans le menu déroulant.
   - Pour créer une nouvelle rubrique, choisissez Créer une nouvelle rubrique. Cela vous amène à la console Amazon SNS où vous pouvez créer une rubrique.
4. Lorsque vous avez terminé, sélectionnez Save.

> **Remarques**
>
> - Vous pouvez utiliser une rubrique SNS standard ou une rubrique SNS FIFO (premier entré, premier sorti). Audit Manager prend en charge l'envoi de notifications aux rubriques FIFO. Cependant, l'ordre dans lequel les messages sont envoyés n'est pas garanti.
> - Si vous voulez utiliser une rubrique Amazon SNS qui ne vous appartient pas, vous devez configurer votre politique (IAM) AWS Identity and Access Management. Plus précisément, vous devez configurer votre politique pour autoriser la publication de la rubrique à partir de l'Amazon Resource Name (ARN). Pour plus d'informations, veuillez consulter la section Gestion des identités et des accès pour AWS Audit Manager.

Résolution des problèmes

Pour trouver des réponses aux questions et problèmes courants, consultez la section Résolution des problèmes de notification dans la section Résolution de ce guide.

Résolution des problèmes dans AWS Audit Manager

Vous pouvez utiliser les informations suivantes pour résoudre les problèmes que vous rencontrez lors de l'utilisation d'AWS Audit Manager.

Si les problèmes que vous rencontrez ne sont pas abordés dans les informations suivantes ou s'ils persistent après que vous avez essayé de les résoudre, veuillez contacter AWS Support.

Rubriques

- Résolution des problèmes liés aux évaluations et à la collecte de preuves
- Résolution des problèmes liés aux rapports d'évaluation
- Résolution des problèmes liés aux contrôles et aux ensembles de contrôles
- Résolution des problèmes liés au tableau de bord
- Résolution des problèmes liés aux administrateurs délégués et à AWS Organizations
- Résolution des problèmes liés à l'outil de recherche de preuves
- Résolution des problèmes liés au partage de cadre
- Résolution des problèmes liés aux notifications
- Résolution des problèmes liés aux autorisations et à l'accès

Résolution des problèmes liés aux évaluations et à la collecte de preuves

Vous pouvez utiliser les informations de cette page pour résoudre les problèmes courants d'évaluation et de collecte de preuves dans Audit Manager.

Rubriques

- J'ai créé une évaluation, mais je ne vois aucune preuve pour le moment
- Mon évaluation ne collecte pas de preuves pour la vérification de la conformité auprès d'AWS Security Hub
- Mon évaluation ne collecte pas de preuves pour la vérification de la conformité auprès d'AWS Config
- Mon évaluation ne collecte pas de preuves de l'activité des utilisateurs auprès d'AWS CloudTrail

- Mon évaluation ne collecte pas de preuves de données de configuration pour un appel d'API AWS
- Mon évaluation ne collecte pas de preuves auprès d'un autre Service AWS
- Mes preuves sont générées à différents intervalles et je ne sais pas à quelle fréquence elles sont collectées
- Que se passe-t-il si je supprime un compte concerné de mon organisation ?
- Je ne parviens pas à modifier les services concernés par mon évaluation
- Quelle est la différence entre un service concerné et un type de source de données ?
- Mon évaluation n'a pas pu être créée
- J'ai désactivé puis réactivé Audit Manager, et à présent, mes évaluations préexistantes ne collectent plus de preuves

J'ai créé une évaluation, mais je ne vois aucune preuve pour le moment

Si vous ne trouvez aucune preuve, il est probable que vous n'ayez pas attendu au moins 24 heures après avoir créé l'évaluation ou qu'il y ait une erreur de configuration.

Nous vous recommandons de contrôler les éléments suivants :

1. Assurez-vous que 24 heures se sont écoulées depuis la création de l'évaluation. Les preuves automatisées sont disponibles 24 heures après la création de l'évaluation.
2. Assurez-vous d'utiliser Audit Manager dans la même Région AWS que le Service AWS dont vous vous attendez à obtenir des preuves.
3. Si vous vous attendez à recevoir des preuves de vérification de la conformité en provenance d'AWS Config et d'AWS Security Hub, assurez-vous que les consoles AWS Config et Security Hub affichent les résultats de ces vérifications. Les résultats d'AWS Config et de Security Hub doivent s'afficher dans la même Région AWS que celle dans laquelle vous utilisez Audit Manager.

Si vous n'observez toujours aucune preuve dans votre évaluation et que cela n'est pas dû à l'un de ces problèmes, vérifiez les autres causes potentielles décrites sur cette page.

Mon évaluation ne collecte pas de preuves pour la vérification de la conformité auprès d'AWS Security Hub

Si vous n'obtenez aucune preuve attestant d'une vérification de la conformité pour un contrôle d'AWS Security Hub, cela peut être dû à l'un des problèmes suivants.

Configuration manquante dans AWS Security Hub

Ce problème peut être dû au fait que vous ayez manqué certaines étapes de configuration lors de l'activation d'AWS Security Hub.

Assurez-vous d'avoir activé Security Hub et configuré vos paramètres comme suit.

Confirmation de vos paramètres Security Hub pour un seul Compte AWS

Si vous utilisez un seul Compte AWS, vérifiez les points suivants :

- Vérifiez que vous avez activé AWS Config et configuré l'enregistrement des ressources pour votre compte.
- Vérifiez que vous avez activé la norme de sécurité PCI DSS pour votre compte.
- Vérifiez que vous avez activé le paramètre de résultats de contrôle consolidés dans Security Hub.

Confirmation de vos paramètres Security Hub pour une organisation

Si vous utilisez des organisations, vérifiez les points suivants :

- Vérifiez que vous avez activé AWS Config et configuré l'enregistrement des ressources pour votre organisation.
- Vérifiez que vous avez activé la norme de sécurité PCI DSS pour chaque compte membre de l'organisation.
- Vérifiez que vous avez activé le paramètre de résultats de contrôle consolidés dans Security Hub.
- Vérifiez que le compte administrateur délégué que vous utilisez dans Security Hub est le même que celui que vous utilisez dans Audit Manager.
- Vérifiez que vous avez activé les comptes de votre organisation en tant que comptes membres de Security Hub.

Un nom de contrôle Security Hub n'a pas été saisi correctement dans votre **`ControlMappingSource`**

Lorsque vous utilisez l'API Audit Manager pour créer un contrôle personnalisé, vous pouvez spécifier un contrôle Security Hub en tant que mappage de source de données pour la collecte de preuves. Pour ce faire, vous devez saisir un identifiant de contrôle en tant que `keywordValue`.

Si vous ne trouvez aucune preuve de vérification de la conformité pour un contrôle Security Hub, il se peut que la `keywordValue` ait été mal saisie dans votre `ControlMappingSource`. La `keywordValue` est sensible à la casse. Si vous ne la saisissez pas correctement, Audit Manager risque de ne pas reconnaître cette règle. Par conséquent, vous risqueriez de ne pas collecter les preuves de vérification de la conformité pour ce contrôle comme prévu.

Pour résoudre ce problème, mettez à jour le contrôle personnalisé et modifiez la `keywordValue`. Le format correct d'un mot clé Security Hub varie. Pour plus de précision, consultez la liste des mots clés de contrôles Security Hub pris en charge.

La règle Amazon EventBridge **`AuditManagerSecurityHubFindingsReceiver`** est manquante

Lorsque vous activez Audit Manager, une règle nommée `AuditManagerSecurityHubFindingsReceiver` est automatiquement créée et activée dans Amazon EventBridge. Cette règle permet à Audit Manager de collecter les résultats de Security Hub à titre de preuve.

Si cette règle n'est pas répertoriée et activée dans la même Région AWS que celle où vous utilisez Security Hub, Audit Manager ne peut pas collecter les résultats de Security Hub pour cette région.

Pour résoudre ce problème, accédez à la console EventBridge et vérifiez que la règle `AuditManagerSecurityHubFindingsReceiver` existe dans votre Compte AWS. Si la règle n'existe pas, nous vous recommandons de désactiver Audit Manager, puis de réactiver le service. Si cette action ne résout pas le problème, ou s'il n'est pas possible de désactiver Audit Manager, contactez AWS Support pour obtenir de l'aide.

Règles AWS Config liées aux services et créées par Security Hub

N'oubliez pas qu'Audit Manager ne collecte pas de preuves en provenance des règles AWS Config liées aux services et créées par Security Hub. Il s'agit d'un type spécifique de règles AWS Config gérées qui est activé et contrôlé par le service Security Hub. Security Hub crée des instances de ces règles liées aux services dans votre environnement AWS, même si d'autres instances des mêmes règles existent déjà. Par conséquent, pour éviter la duplication des preuves, Audit Manager ne prend pas en charge la collecte de preuves en provenance des règles liées aux services.

Mon évaluation ne collecte pas de preuves pour la vérification de la conformité auprès d'AWS Config

Si vous n'obtenez aucune preuve attestant d'une vérification de la conformité pour une règle AWS Config, cela peut être dû à l'un des problèmes suivants.

L'identifiant de règle n'a pas été saisi correctement dans votre **`ControlMappingSource`**

Lorsque vous utilisez l'API Audit Manager pour créer un contrôle personnalisé, vous pouvez spécifier une règle AWS Config en tant que mappage de source de données pour la collecte de preuves. La `keywordValue` que vous spécifiez dépend du type de règle.

Si vous ne trouvez aucune preuve de vérification de la conformité pour une règle AWS Config, il se peut que la `keywordValue` ait été mal saisie dans votre `ControlMappingSource`. La `keywordValue` est sensible à la casse. Si vous ne la saisissez pas correctement, Audit Manager risque de ne pas reconnaître la règle. Par conséquent, vous risqueriez de ne pas collecter les preuves de vérification de la conformité pour cette règle comme prévu.

Pour résoudre ce problème, mettez à jour le contrôle personnalisé et modifiez la `keywordValue`.

- Pour les règles personnalisées, assurez-vous que la `keywordValue` présente le préfixe `Custom_` suivi du nom de la règle personnalisée. Le format du nom de règle personnalisée peut varier. Pour plus de précision, consultez la console AWS Config pour vérifier les noms de vos règles personnalisées.
- Pour les règles gérées, assurez-vous que la `keywordValue` soit l'identifiant de la règle en `ALL_CAPS_WITH_UNDERSCORES`. Par exemple, `CLOUDWATCH_LOG_GROUP_ENCRYPTED`. Pour plus de précision, consultez la liste des mots clés de règles gérées pris en charge.

> **Note**
>
> Pour certaines règles gérées, l'identifiant de la règle est différent du nom de la règle. Par exemple, l'identifiant de la règle pour restricted-ssh est `INCOMING_SSH_DISABLED`. Assurez-vous d'utiliser l'identifiant de la règle, et non le nom de la règle. Pour trouver un identifiant de règle, choisissez une règle dans la liste des règles gérées et recherchez sa valeur Identifiant.

La règle est une règle AWS Config liée à un service

Vous pouvez utiliser des règles gérées et des règles personnalisées en tant que mappage de source de données pour la collecte de preuves. Cependant, Audit Manager ne collecte pas de preuves en provenance de la plupart des règles liées aux services.

Il n'existe que deux types de règles liées aux services à partir desquels Audit Manager peut collecter des preuves :

- Règles liées aux services issues des packs de conformité
- Règles liées aux services provenant d'AWS Organizations

Audit Manager ne collecte pas de preuves à partir d'autres règles liées aux services, en particulier des règles comportant un Amazon Resource Name (ARN) contenant le préfixe suivant : `arn:aws:config:*:*:config-rule/aws-service-rule/...`

Audit Manager ne collecte pas de preuves dans le cadre de la plupart des règles AWS Config liées aux services afin d'éviter la duplication des preuves dans vos évaluations. Une règle liée à un service est un type spécifique de règle gérée qui prend en charge d'autres Services AWS pour créer des règles AWS Config dans votre compte. Par exemple, certains contrôles Security Hub utilisent une règle AWS Config liée à un service pour exécuter des contrôles de sécurité. Pour chaque contrôle Security Hub qui utilise une règle AWS Config liée à un service, Security Hub crée une instance de la règle AWS Config requise dans votre environnement AWS. Cela se produit même si la règle d'origine existe déjà dans votre compte. Par conséquent, pour éviter de collecter deux fois les mêmes preuves à partir de la même règle, Audit Manager ignore la règle liée au service et ne collecte aucune preuve à partir de celle-ci.

AWS Config n'est pas activé et inclus en tant que service concerné

AWS Config doit être activé dans votre Compte AWS. Il doit également être inclus en tant que service dans le cadre de votre évaluation. Une fois qu'AWS Config a été configuré, Audit Manager collecte des preuves à chaque fois que l'évaluation d'une règle AWS Config a lieu.

Tout d'abord, assurez-vous que vous avez activé AWS Config dans votre Compte AWS. Pour obtenir des instructions, consultez Enable and set up AWS Config.

Ensuite, assurez-vous que vous avez inclus AWS Config en tant que service dans le cadre de votre évaluation. Pour consulter les services actuellement concernés par votre évaluation, rendez-vous sur Review an assessment, onglet Services AWS. Pour modifier la liste des services concernés par une évaluation, consultez Edit Services AWS in scope.

La règle AWS Config a évalué une configuration de ressources avant que vous ayez configuré votre évaluation

Si votre règle AWS Config est configurée pour évaluer les modifications de configuration d'une ressource spécifique, il se peut que vous constatiez un décalage entre l'évaluation dans AWS Config et les preuves dans Audit Manager. Cela se produit si l'évaluation des règles a eu lieu avant que vous ne configuriez le contrôle dans votre évaluation Audit Manager. Dans ce cas, Audit Manager ne génère de preuves que lorsque la ressource sous-jacente change à nouveau de statut et déclenche une réévaluation de la règle.

Pour contourner le problème, vous pouvez accéder à la règle dans la console AWS Config et la réévaluer manuellement. Cela implique une nouvelle évaluation de toutes les ressources relatives à cette règle.

Mon évaluation ne collecte pas de preuves de l'activité des utilisateurs auprès d'AWS CloudTrail

Lorsque vous utilisez l'API Audit Manager pour créer un contrôle personnalisé, vous pouvez spécifier un nom d'événement CloudTrail en tant que mappage de source de données pour la collecte de preuves. Pour ce faire, vous devez saisir le nom de l'événement en tant que `keywordValue`.

Si vous ne trouvez aucune preuve de l'activité des utilisateurs pour un événement CloudTrail, il se peut que la `keywordValue` ait été mal saisie dans votre `ControlMappingSource`. La `keywordValue` est sensible à la casse. Si vous ne la saisissez pas correctement, Audit Manager risque de ne pas reconnaître le nom de l'événement. Par conséquent, vous risqueriez de ne pas collecter les preuves de l'activité des utilisateurs pour cet événement comme prévu.

Pour résoudre ce problème, mettez à jour le contrôle personnalisé et modifiez la `keywordValue`. Assurez-vous que l'événement est écrit sous la forme `serviceprefix_ActionName`. Par exemple, `cloudtrail_StartLogging`. Pour plus de précision, vérifiez le préfixe Service AWS et les noms des actions dans la Référence de l'autorisation de service.

Mon évaluation ne collecte pas de preuves de données de configuration pour un appel d'API AWS

Lorsque vous utilisez l'API Audit Manager pour créer un contrôle personnalisé, vous pouvez spécifier un appel d'API AWS en tant que mappage de source de données pour la collecte de preuves. Pour ce faire, vous devez saisir l'appel d'API en tant que `keywordValue`.

Si vous ne trouvez aucune preuve de données de configuration pour un appel d'API AWS, il se peut que la `keywordValue` ait été mal saisie dans votre `ControlMappingSource`. La `keywordValue` est sensible à la casse. Si vous ne la saisissez pas correctement, Audit Manager risque de ne pas reconnaître l'appel d'API. Par conséquent, vous risqueriez de ne pas collecter les preuves des données de configuration pour cet appel d'API comme prévu.

Pour résoudre ce problème, mettez à jour le contrôle personnalisé et modifiez la `keywordValue`. Assurez-vous que l'appel d'API est écrit sous la forme `serviceprefix_ActionName`. Par exemple, `iam_ListGroups`. Pour plus de précision, consultez la liste des appels d'API pris en charge.

Mon évaluation ne collecte pas de preuves auprès d'un autre Service AWS

Si aucun Service AWS n'est sélectionné dans le cadre de votre évaluation, Audit Manager ne collecte pas de preuves auprès des ressources liées à ce service. C'est également le cas si un Service AWS est sélectionné mais que vous ne l'avez pas activé dans votre environnement.

Si vous avez créé votre évaluation à partir d'un cadre personnalisé, vous pouvez modifier les services concernés par votre évaluation. Vous pouvez ensuite spécifier les Services AWS supplémentaires à partir desquels vous souhaitez collecter des preuves. Une fois que vous avez ajouté ces services, les preuves sont disponibles sous 24 heures.

> **Note**
>
> Si vous avez créé votre évaluation à partir d'un cadre standard, la liste des Services AWS concernés est présélectionnée et ne peut pas être modifiée. En effet, lorsque vous créez une évaluation à partir d'un cadre standard, Audit Manager mappe et sélectionne automatiquement les sources de données et les services appropriés pour vous. La sélection est effectuée en fonction des exigences du cadre standard. Notez que pour les cadres standard contenant uniquement des contrôles manuels, aucun Services AWS n'est concerné. La solution pour modifier les Services AWS concernés tout en créant une évaluation basée sur un cadre standard consiste à personnaliser le cadre standard. En utilisant cette solution de contournement, vous pouvez utiliser le cadre que vous avez personnalisé pour créer une nouvelle évaluation. Dans le cadre de cette évaluation, vous pouvez ensuite spécifier les Services AWS concernés.

Mes preuves sont générées à différents intervalles et je ne sais pas à quelle fréquence elles sont collectées

Les contrôles des évaluations d'Audit Manager sont mappés à différentes sources de données. Chaque source de données possède une fréquence de collecte de preuves différente. Par conséquent, il n'existe pas de réponse universelle quant à la fréquence à laquelle les preuves sont collectées. Certaines sources de données évaluent la conformité, tandis que d'autres ne capturent que le statut des ressources et les données de modification sans détermination de la conformité.

Vous trouverez ci-dessous un résumé des différents types de sources de données et de la fréquence à laquelle elles collectent des preuves.

Type de source de données	Description	Fréquence de collecte des preuves	Lorsque ce contrôle est actif dans une évaluation
AWS CloudTrail	Suit l'activité d'un utilisateur spécifique.	En continu	Audit Manager filtre vos journaux CloudTrail en fonction du mot clé que vous choisissez. Les journaux traités sont importés en tant que preuves de l'activité de l'utilisateur.
AWS Security Hub	Capture un instantané du niveau de sécurité de vos ressources en rapportant les résultats de Security Hub.	Selon le calendrier de vérification de Security Hub (généralement toutes les 12 heures environ)	Audit Manager récupère le résultat de sécurité directement depuis Security Hub. Le résultat est importé en tant que preuve de contrôle de la conformité.
AWS Config	Capture un instantané du niveau de sécurité de vos ressources en rapportant les	Selon les paramètres définis dans la règle AWS Config	Audit Manager récupère l'évaluation des règles directement à partir d'AWS Config. L'évaluation est importée en tant que preuve de contrôle de la conformité.

Type de source de données	Description	Fréquence de collecte des preuves	Lorsque ce contrôle est actif dans une évaluation
	résultats d'AWS Config.		
Appels d'API AWS	Prend un instantané de la configuration de vos ressources directement par le biais d'un appel d'API au Service AWS indiqué.	Tous les jours, toutes les semaines ou tous les mois	Audit Manager effectue l'appel d'API en fonction de la fréquence que vous spécifiez. La réponse est importée en tant que preuve des données de configuration.

Quelle que soit la fréquence de collecte des preuves, les nouvelles preuves sont collectées automatiquement tant que l'évaluation est active. Pour plus d'informations, consultez Evidence collection frequency.

Pour en savoir plus, consultez Supported control data sources for automated evidence et Changing the evidence collection frequency for a control.

Que se passe-t-il si je supprime un compte concerné de mon organisation ?

Lorsqu'un compte concerné est supprimé de votre organisation, Audit Manager ne collecte plus de preuves pour ce compte. Cependant, le compte continue d'apparaître dans votre évaluation sous l'onglet Comptes AWS. Pour supprimer le compte de la liste des comptes concernés, modifiez l'évaluation. Le compte supprimé n'apparaît plus dans la liste lors de la modification et vous pouvez enregistrer vos modifications sans que ce compte soit concerné.

Je ne parviens pas à modifier les services concernés par mon évaluation

Lorsque vous utilisez la console Audit Manager pour créer une évaluation à partir d'un cadre standard, la liste des Services AWS concernés est sélectionnée par défaut. Cette liste ne peut pas être modifiée. En effet, Audit Manager mappe et sélectionne automatiquement les sources de données et les services pour vous. Cette sélection est effectuée conformément aux exigences du framework standard. Si le cadre standard que vous avez sélectionné ne contient que des contrôles

manuels, aucun Services AWS n'est concerné dans votre évaluation et vous ne pouvez ajouter aucun service à votre évaluation.

Si vous devez modifier la liste des services concernés, utilisez l'opération d'API UpdateAssessment fournie par Audit Manager. Vous pouvez également personnaliser le framework standard, puis créer une évaluation à partir du framework personnalisé.

Quelle est la différence entre un service concerné et un type de source de données ?

Un service concerné est un Service AWS spécifié dans le cadre de votre évaluation. Lorsqu'un service est concerné, Audit Manager collecte des preuves concernant votre utilisation de ce service et de ses ressources.

Un type de source de données indique d'où proviennent exactement les preuves. Si vous chargez vos propres preuves, le type de source de données est Manuel. Si Audit Manager collecte les preuves, la source de données peut être de quatre types.

1. AWS Security Hub : capture un instantané du niveau de sécurité de vos ressources en rapportant les résultats de Security Hub.
2. AWS Config : capture un instantané du niveau de sécurité de vos ressources en rapportant les résultats d'AWS Config.
3. AWS CloudTrail : suit l'activité d'un utilisateur spécifique pour une ressource.
4. Appels d'API AWS : prend un instantané de la configuration de vos ressources directement par le biais d'un appel d'API à un Service AWS spécifique.

Voici deux exemples illustrant la différence entre un service concerné et le type de source de données.

Exemple 1

Supposons que vous souhaitiez collecter des preuves pour un contrôle nommé 4.1.2 - Interdire l'accès en écriture public aux compartiments S3. Ce contrôle vérifie les niveaux d'accès de vos politiques de compartiment S3. Pour ce contrôle, Audit Manager utilise une règle AWS Config spécifique (s3-bucket-public-write-prohibited) pour rechercher une évaluation de vos compartiments S3. Dans cet exemple, les conditions suivantes sont remplies :

- Le service concerné est Amazon S3

- Les ressources en cours d'évaluation sont vos compartiments S3
- Le type de source de données est AWS Config
- Le mappage de source de données est une règle AWS Config spécifique (`s3-bucket-public-write-prohibited`)

Exemple 2

Supposons que vous souhaitiez collecter des preuves pour un contrôle HIPAA nommé 164.308(a)(5)(ii)(C). Ce contrôle nécessite une procédure de surveillance pour détecter les connexions inappropriées. Pour ce contrôle, Audit Manager utilise les journaux CloudTrail pour rechercher tous les événements de connexion à la Console de gestion AWS. Dans cet exemple, les conditions suivantes sont remplies :

- Le service concerné est IAM
- Les ressources en cours d'évaluation sont vos utilisateurs
- Le type de source de données est CloudTrail
- Le mappage de source de données est un événement CloudTrail spécifique (`ConsoleLogin`)

Mon évaluation n'a pas pu être créée

Si la création de votre évaluation échoue, c'est peut-être parce que vous avez sélectionné un trop grand nombre d'Comptes AWS dans le cadre de votre évaluation. Si vous utilisez AWS Organizations, Audit Manager peut prendre en charge 150 comptes membres maximum dans le cadre d'une seule évaluation. Si vous dépassez ce nombre, la création de l'évaluation risque d'échouer. Pour contourner le problème, vous pouvez exécuter plusieurs évaluations avec différents comptes dans le cadre de chaque évaluation.

J'ai désactivé puis réactivé Audit Manager, et à présent, mes évaluations préexistantes ne collectent plus de preuves

Lorsque vous désactivez Audit Manager et que vous choisissez de ne pas supprimer vos données, vos évaluations existantes passent au statut inactif et cessent de collecter des preuves. Cela signifie que lorsque vous réactivez Audit Manager, les évaluations que vous avez créées précédemment restent disponibles. Cependant, elles ne reprennent pas automatiquement la collecte de preuves.

Pour qu'une évaluation préexistante recommence à collecter des preuves, modifiez l'évaluation et choisissez Enregistrer sans apporter de modifications.

Résolution des problèmes liés aux rapports d'évaluation

Vous pouvez utiliser les informations de cette page pour résoudre les problèmes courants liés aux rapports d'évaluation dans Audit Manager.

Rubriques

- Mon rapport d'évaluation n'a pas pu être généré
- J'ai suivi la liste de contrôle ci-dessus et mon rapport d'évaluation n'a toujours pas été généré
- Je reçois un message d'erreur d'accès refusé lorsque j'essaie de générer un rapport
- Je ne suis pas en mesure de décompresser le rapport d'évaluation
- Lorsque je choisis le nom d'une preuve dans un rapport, je ne suis pas redirigé vers les détails de la preuve
- La génération de mon rapport d'évaluation est bloquée au statut En cours, et je ne sais pas quelles répercussions cela aura sur ma facturation
- Voir aussi

Mon rapport d'évaluation n'a pas pu être généré

Votre rapport d'évaluation n'a peut-être pas été généré pour plusieurs raisons. Vous pouvez commencer à résoudre ce problème en vérifiant les causes les plus fréquentes. Utilisez la liste de contrôle suivante pour commencer.

1. Vérifiez si certaines de vos informations en matière d'Région AWS ne concordent pas :
   a. L'Région AWS de la clé gérée par votre client correspond-elle à l'Région AWS de votre évaluation ?

      Si vous avez fourni votre propre clé KMS pour le chiffrement des données Audit Manager, la clé doit se trouver dans la même Région AWS que celle de votre évaluation. Pour résoudre ce problème, remplacez la clé KMS par une clé située dans la même région que votre évaluation. Pour obtenir des instructions sur la modification de la clé KMS, consultez AWS Audit Manager Paramètres, Chiffrement des données.
   b. L'Région AWS de la clé gérée par votre client correspond-elle à l'Région AWS de votre compartiment S3 ?

Si vous avez fourni votre propre clé KMS pour le chiffrement des données Audit Manager, la clé doit se trouver dans la même Région AWS que celle du compartiment S3 que vous utilisez comme destination de votre rapport d'évaluation. Pour résoudre ce problème, vous pouvez modifier la clé KMS ou le compartiment S3 afin qu'ils se trouvent tous les deux dans la même région que votre évaluation. Pour obtenir des instructions sur la modification de la clé KMS, consultez AWS Audit Manager Paramètres, Chiffrement des données. Pour obtenir des instructions sur la modification du compartiment S3, consultez AWS Audit Manager Paramètres, Destination du rapport d'évaluation.

2. Vérifiez les autorisations du compartiment S3 que vous utilisez comme destination du rapport d'évaluation :

   a. L'entité IAM qui génère le rapport d'évaluation possède-t-elle les autorisations nécessaires pour le compartiment S3 ?

      L'entité IAM doit disposer des autorisations nécessaires concernant le compartiment S3 afin de publier des rapports dans ce compartiment. Nous fournissons un exemple de politique que vous pouvez utiliser. Pour obtenir des instructions sur la spécification d'un compartiment S3 différent, consultez AWS Audit Manager settings, Assessment report destination.

   b. Le compartiment S3 dispose-t-il d'une politique de compartiment qui exige un chiffrement côté serveur (SSE) utilisant SSE-KMS ?

      Si oui, la clé KMS utilisée dans cette politique de compartiment doit correspondre à la clé KMS spécifiée dans vos paramètres de chiffrement des données Audit Manager. Si vous n'avez pas configuré de clé KMS dans vos paramètres Audit Manager et que votre politique de compartiment S3 nécessite SSE, assurez-vous que la politique de compartiment autorise SSE-S3. Pour obtenir des instructions sur la modification de la clé KMS, consultez AWS Audit Manager Paramètres, Chiffrement des données. Pour obtenir des instructions sur la modification du compartiment S3, consultez AWS Audit Manager Paramètres, Destination du rapport d'évaluation.

Si vous ne parvenez toujours pas à générer un rapport d'évaluation, passez en revue les problèmes suivants sur cette page.

J'ai suivi la liste de contrôle ci-dessus et mon rapport d'évaluation n'a toujours pas été généré

Audit Manager limite la quantité de preuves que vous pouvez ajouter à un rapport d'évaluation. La limite dépend de l'Région AWS de votre évaluation, de la région du compartiment S3 utilisé comme destination de votre rapport d'évaluation et du fait que votre évaluation utilise ou non une AWS KMS key gérée par le client.

1. La limite est de 22 000 pour les rapports d'une même région (dans le cas où le compartiment S3 et l'évaluation se trouvent dans la même Région AWS)
2. La limite est de 3 500 pour les rapports interrégionaux (dans le cas où le compartiment S3 et l'évaluation se trouvent dans des Régions AWS différentes)
3. La limite est de 3 500 si l'évaluation utilise une clé KMS gérée par le client

Si vous essayez de générer un rapport contenant plus de preuves que les limites susmentionnées, l'opération risque d'échouer.

Pour contourner le problème, vous pouvez générer plusieurs rapports d'évaluation plutôt qu'un seul rapport d'évaluation plus volumineux. Ce faisant, vous pouvez exporter les preuves de votre évaluation vers des lots dont la taille est davantage gérable.

Je reçois un message d'erreur d'accès refusé lorsque j'essaie de générer un rapport

Vous recevrez un message d'erreur `access denied` si votre évaluation a été créée par un compte administrateur délégué auquel la clé KMS spécifiée dans vos paramètres Audit Manager n'appartient pas. Pour éviter cette erreur, lorsque vous désignez un administrateur délégué pour Audit Manager, assurez-vous que le compte administrateur délégué a accès à la clé KMS que vous avez fournie lors de la configuration d'Audit Manager.

Vous pouvez également recevoir un message d'erreur `access denied` si vous ne disposez pas des autorisations d'écriture pour le compartiment S3 que vous utilisez comme destination de votre rapport d'évaluation.

Si vous recevez un message d'erreur `access denied`, veillez à respecter les exigences suivantes :

- Votre clé KMS dans vos paramètres Audit Manager donne des autorisations à l'administrateur délégué. Vous pouvez configurer ceci en suivant les instructions de la section Autoriser des

utilisateurs d'autres comptes à utiliser une clé KMS dans le Guide du développeur d'AWS Key Management Service. Pour obtenir des instructions sur la vérification et la modification de vos paramètres de chiffrement dans Audit Manager, consultez Data encryption.

- Vous disposez d'une politique d'autorisation qui vous accorde un accès en écriture au compartiment S3 que vous utilisez comme destination du rapport d'évaluation. Plus précisément, votre politique d'autorisation contient une action `s3:PutObject`, spécifie l'ARN du compartiment S3 et inclut la clé KMS utilisée pour chiffrer vos rapports d'évaluation. Pour un exemple de politique que vous pouvez utiliser, consultez Identity-based policy examples for AWS Audit Manager.

> **Note**
>
> Si vous modifiez vos paramètres de chiffrement des données dans Audit Manager, ces modifications s'appliqueront aux nouvelles évaluations que vous créerez à l'avenir. Cela inclut tous les rapports d'évaluation que vous créez à partir de vos nouvelles évaluations.
> Les modifications ne s'appliquent pas aux évaluations existantes que vous avez créées avant de modifier vos paramètres de chiffrement. Cela inclut les nouveaux rapports d'évaluation que vous créez à partir d'évaluations existantes, en plus des rapports d'évaluation existants.
> Les évaluations existantes, ainsi que tous leurs rapports d'évaluation, continuent d'utiliser l'ancienne clé KMS. Si l'identité IAM qui génère le rapport d'évaluation n'est pas autorisée à utiliser l'ancienne clé KMS, vous pouvez accorder des autorisations au niveau de la stratégie de clé.

Je ne suis pas en mesure de décompresser le rapport d'évaluation

Si vous ne parvenez pas à décompresser le rapport d'évaluation sous Windows, il est probable que Windows Explorer ne puisse pas l'extraire, car son chemin de fichier comporte plusieurs dossiers imbriqués ou des noms longs. Cela est dû au fait que, dans le système de dénomination des fichiers Windows, le chemin du dossier, le nom du fichier et l'extension du fichier ne peuvent pas dépasser 259 caractères. Dans le cas contraire, cela entraîne un message d'erreur `Destination Path Too Long`.

Pour résoudre ce problème, essayez de déplacer le fichier zip vers le dossier parent de son emplacement actuel. Vous pouvez ensuite réessayer de le décompresser à partir de cet endroit. Vous pouvez également essayer de raccourcir le nom du fichier zip ou de l'extraire vers un autre emplacement dont le chemin de fichier est plus court.

Lorsque je choisis le nom d'une preuve dans un rapport, je ne suis pas redirigé vers les détails de la preuve

Ce problème peut se produire si vous interagissez avec le rapport d'évaluation dans un navigateur ou si vous utilisez le lecteur PDF par défaut installé sur votre système d'exploitation. Certains lecteurs PDF par défaut du navigateur et du système n'autorisent pas l'ouverture de liens relatifs. En d'autres termes, bien que les hyperliens puissent fonctionner dans le résumé PDF du rapport d'évaluation (comme les noms des contrôles liés par des hyperliens dans la table des matières), les hyperliens sont ignorés lorsque vous essayez de quitter le résumé PDF de l'évaluation pour passer à un PDF détaillé des preuves distinct.

Si vous rencontrez ce problème, nous vous recommandons d'utiliser un lecteur PDF dédié pour interagir avec vos rapports d'évaluation. Pour une expérience fiable, nous vous recommandons d'installer et d'utiliser Adobe Acrobat Reader, que vous pouvez télécharger sur le site Web d'Adobe. D'autres lecteurs PDF sont également disponibles, mais il a été prouvé qu'Adobe Acrobat Reader fonctionne de manière cohérente et fiable avec les rapports d'évaluation d'Audit Manager.

La génération de mon rapport d'évaluation est bloquée au statut En cours, et je ne sais pas quelles répercussions cela aura sur ma facturation

La génération du rapport d'évaluation n'a aucune répercussion sur la facturation. Vous êtes facturé uniquement en fonction des preuves collectées dans le cadre de vos évaluations. Pour plus d'informations sur la tarification, consultez Tarification d'AWS Audit Manager.

Voir aussi

Les pages suivantes contiennent des conseils pour la résolution des problèmes liés à la génération d'un rapport d'évaluation à partir de l'outil de recherche de preuves :

- Je ne parviens pas à générer plusieurs rapports d'évaluation à partir des résultats de ma recherche
- Je ne parviens pas à ajouter des résultats de recherche individuels à un rapport d'évaluation
- Les résultats de ma recherche de preuves ne sont pas tous inclus dans le rapport d'évaluation
- Je souhaite générer un rapport d'évaluation à partir des résultats de ma recherche, mais mon instruction de requête échoue

Résolution des problèmes liés aux contrôles et aux ensembles de contrôles

Vous pouvez utiliser les informations de cette page pour résoudre les problèmes courants liés aux contrôles dans Audit Manager.

Problèmes généraux

- Je ne vois aucun contrôle ou ensemble de contrôles dans mon évaluation
- Je ne parviens pas à charger des preuves manuelles dans un contrôle

Problèmes d'intégration d'AWS Config

- Je dois utiliser plusieurs règles AWS Config comme source de données pour un contrôle unique
- L'option de règle personnalisée n'est pas disponible lorsque je configure une source de données pour un contrôle
- L'option de règle personnalisée est disponible, mais aucune règle n'apparaît dans la liste déroulante
- Certaines règles personnalisées sont disponibles, mais je ne vois pas la règle que je souhaite utiliser
- Je ne vois pas la règle gérée que je souhaite utiliser
- Je souhaite partager un cadre personnalisé, mais il comporte des contrôles qui utilisent des règles AWS Config personnalisées comme source de données. Le destinataire peut-il collecter des preuves pour ces contrôles ?
- Que se passe-t-il lorsqu'une règle personnalisée est mise à jour dans AWS Config ? Dois-je prendre des mesures dans Audit Manager ?

Je ne vois aucun contrôle ou ensemble de contrôles dans mon évaluation

En bref, pour consulter les contrôles d'une évaluation, vous devez être désigné comme responsable de l'audit de l'évaluation en question. En outre, vous devez disposer des autorisations IAM nécessaires pour consulter et gérer les ressources d'Audit Manager associées.

Si vous avez besoin d'accéder aux contrôles d'une évaluation, demandez à l'un des responsables de l'audit de vous désigner comme responsable de l'audit. Vous pouvez désigner les responsables de l'audit lorsque vous créez ou modifiez une évaluation.

Vérifiez également que vous disposez des autorisations nécessaires pour gérer l'évaluation. Nous recommandons aux responsables de l'audit d'utiliser la politique AWSAuditManagerAdministratorAccess. Si vous avez besoin d'aide concernant les autorisations IAM, contactez votre administrateur ou AWS Support. Pour plus d'informations sur l'attachement d'une politique à une identité IAM, consultez Ajout d'autorisations à un utilisateur et Ajout et suppression d'autorisations basées sur l'identité IAM dans le Guide de l'utilisateur IAM.

Je ne parviens pas à charger des preuves manuelles dans un contrôle

Si vous ne pouvez pas charger manuellement des preuves dans un contrôle, c'est probablement parce que le statut du contrôle est inactif.

Pour charger des preuves manuelles dans un contrôle, vous devez d'abord faire passer le statut du contrôle sur En cours de vérification ou Vérifié. Pour plus d'informations, consultez Update control status.

> **Important**
>
> Chaque Compte AWS ne peut charger manuellement que 100 fichiers de preuves maximum dans un contrôle par jour. Le dépassement de ce quota quotidien entraîne l'échec de tout chargement manuel supplémentaire pour le contrôle en question. Si vous devez charger une grande quantité de preuves manuelles dans un seul contrôle, chargez-les par lots sur plusieurs jours.

Je dois utiliser plusieurs règles AWS Config comme source de données pour un contrôle unique

Vous pouvez utiliser une combinaison de règles gérées et de règles personnalisées pour un seul contrôle. Pour ce faire, configurez plusieurs sources de données pour le contrôle et sélectionnez le type de règle que vous préférez pour chacune d'entre elles. Vous pouvez définir 10 sources de données maximum pour un seul contrôle personnalisé.

L'option de règle personnalisée n'est pas disponible lorsque je configure une source de données pour un contrôle

Cela signifie que vous n'êtes pas autorisé à consulter les règles personnalisées de votre Compte AWS ou de votre organisation. Plus précisément, vous n'êtes pas autorisé à effectuer l'opération DescribeConfigRules dans la console Audit Manager.

Pour résoudre ce problème, contactez votre administrateur AWS pour obtenir de l'aide. Si vous êtes un administrateur AWS, vous pouvez accorder des autorisations à vos utilisateurs ou à vos groupes en gérant vos politiques IAM.

L'option de règle personnalisée est disponible, mais aucune règle n'apparaît dans la liste déroulante

Cela signifie qu'aucune règle personnalisée n'est activée et ne peut être utilisée dans votre Compte AWS ou dans votre organisation.

Si vous n'avez pas encore de règles personnalisées dans AWS Config, vous pouvez en créer une. Pour obtenir des instructions, consultez AWS Config custom rules dans le Guide du développeur d'AWS Config.

Si vous vous attendez à voir une règle personnalisée, consultez l'élément de résolution des problèmes suivant.

Certaines règles personnalisées sont disponibles, mais je ne vois pas la règle que je souhaite utiliser

Si vous ne voyez pas la règle personnalisée que vous vous attendez à trouver, cela peut être dû à l'un des problèmes suivants.

Votre compte est exclu de la règle

Il est possible que le compte administrateur délégué que vous utilisez soit exclu de la règle.

Le compte de gestion de votre organisation (ou l'un des comptes administrateurs délégués AWS Config) peut créer des règles d'organisation personnalisées à l'aide de l'AWS Command Line Interface (AWS CLI). Lorsque tel est le cas, il peut spécifier une liste de comptes à exclure de la règle. Si votre compte figure dans cette liste, la règle n'est pas disponible dans Audit Manager.

Pour résoudre ce problème, contactez votre administrateur AWS Config pour obtenir de l'aide. Si vous êtes un administrateur AWS Config, vous pouvez mettre à jour la liste des comptes exclus en exécutant la commande put-organization-config-rule.

La règle n'a pas été correctement créée et activée dans AWS Config

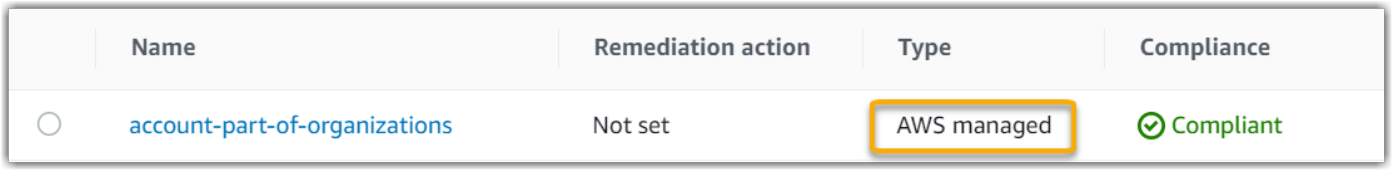
Il est également possible que la règle personnalisée n'ait pas été créée et activée correctement. Si une erreur s'est produite lors de la création de la règle ou si la règle n'est pas activée, elle n'apparaît pas dans la liste des règles disponibles dans Audit Manager.

Pour obtenir de l'aide à ce sujet, nous vous recommandons de contacter votre administrateur AWS Config.

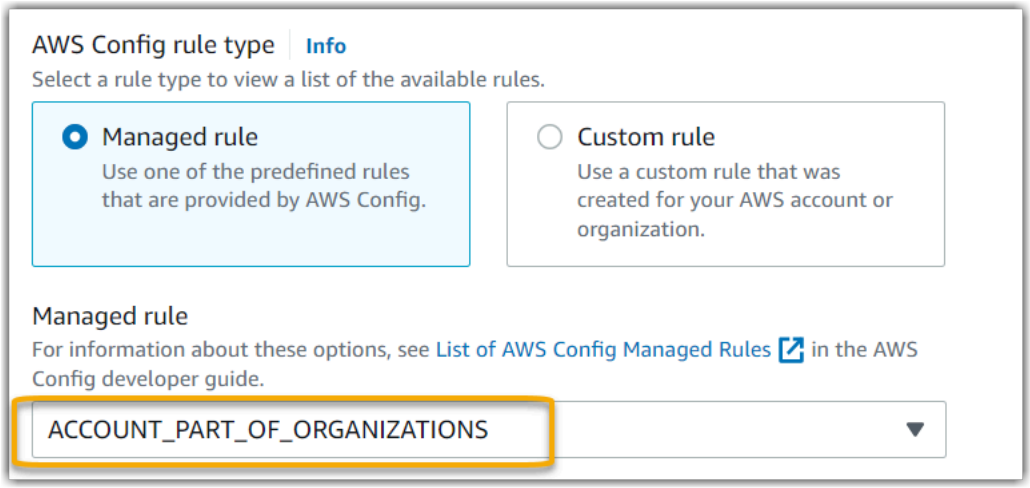
La règle est une règle gérée

Si vous ne trouvez pas la règle que vous recherchez dans la liste déroulante des règles personnalisées, il est possible qu'il s'agisse d'une règle gérée.

Vous pouvez utiliser la console AWS Config pour vérifier si une règle est une règle gérée. Pour ce faire, choisissez Règles dans le menu de navigation de gauche et recherchez la règle dans le tableau. S'il s'agit d'une règle gérée, la colonne Type indique Gérée par AWS.

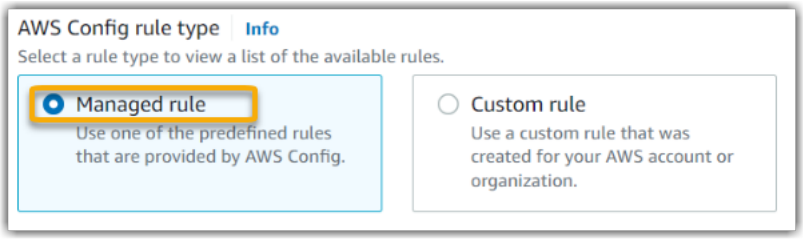


Après avoir vérifié qu'il s'agit d'une règle gérée, revenez dans Audit Manager et sélectionnez Règle gérée comme type de règle. Recherchez ensuite le mot clé identifiant de la règle gérée dans la liste déroulante des règles gérées.



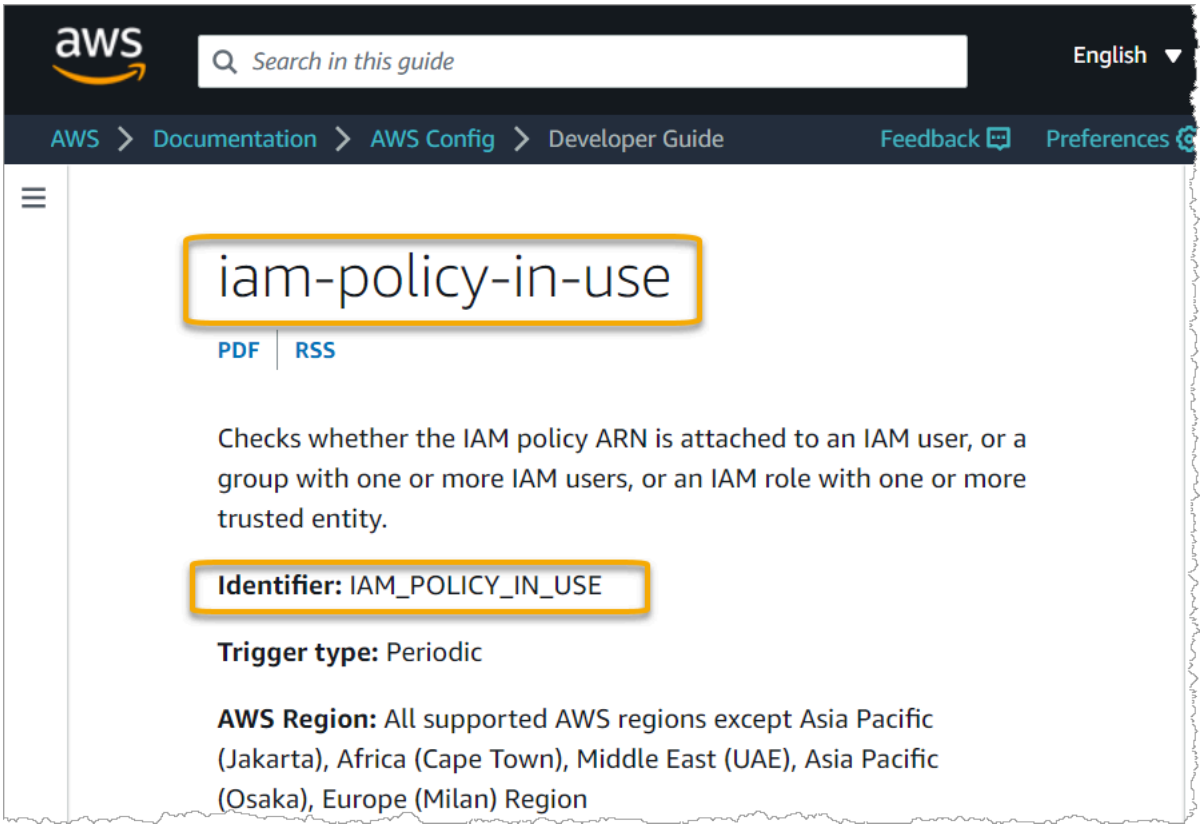
Je ne vois pas la règle gérée que je souhaite utiliser

Avant de sélectionner une règle dans la liste déroulante de la console Audit Manager, assurez-vous d'avoir sélectionné Règle gérée comme type de règle.

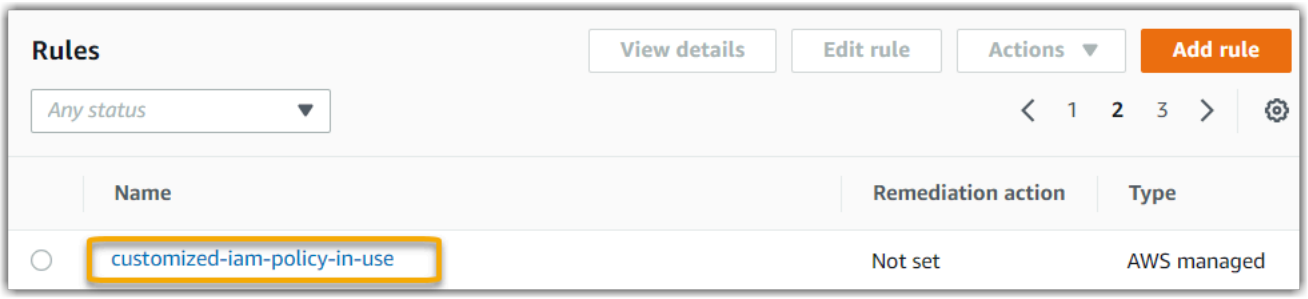


Si vous ne voyez toujours pas la règle gérée que vous vous attendez à trouver, il est possible que vous recherchiez le nom de la règle. Vous devez plutôt rechercher l'identifiant de la règle.

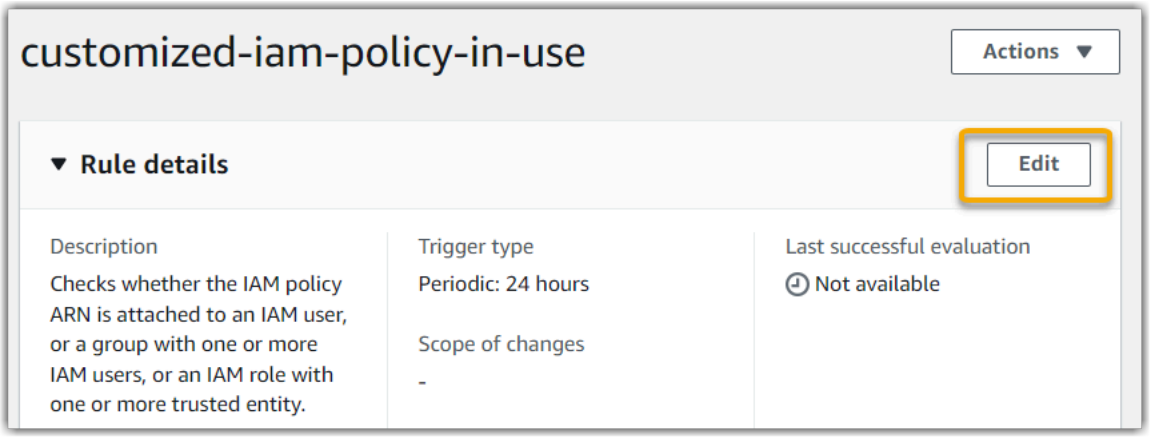
Si vous utilisez une règle gérée par défaut, le nom et l'identifiant sont similaires. Le nom est en minuscules et utilise des tirets (par exemple, `iam-policy-in-use`). L'identifiant est en majuscules et utilise des traits de soulignement (par exemple, `IAM_POLICY_IN_USE`). Pour trouver l'identifiant d'une règle gérée par défaut, consultez la liste des mots clés de règles gérées AWS Config pris en charge et suivez le lien de la règle que vous souhaitez utiliser. Vous accédez ainsi à la documentation AWS Config relative à cette règle gérée. À partir de là, vous pouvez voir à la fois le nom et l'identifiant. Recherchez le mot clé identifiant dans la liste déroulante d'Audit Manager.



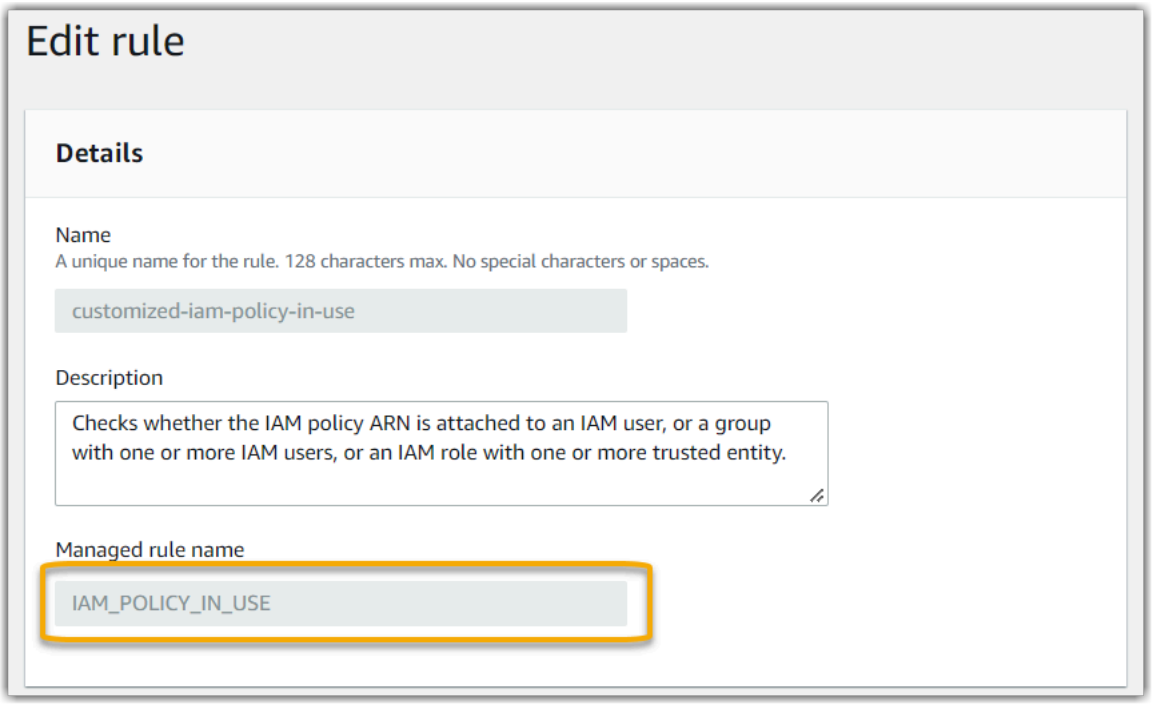
Si vous utilisez une règle gérée personnalisée, vous pouvez utiliser la console AWS Config pour trouver l'identifiant de la règle. Par exemple, supposons que vous souhaitiez utiliser la règle gérée appelée `customized-iam-policy-in-use`. Pour trouver l'identifiant de cette règle, accédez à la console AWS Config, choisissez Règles dans le menu de navigation de gauche, puis choisissez la règle dans le tableau.



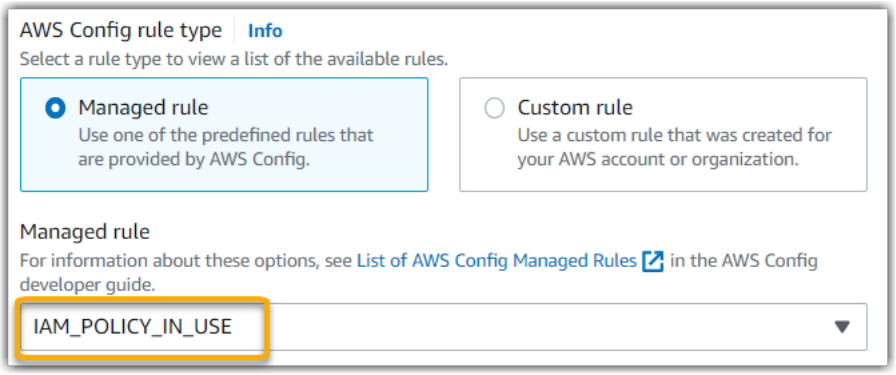
Choisissez Modifier pour afficher les détails de la règle gérée.



Dans la section Détails, vous pouvez trouver l'identifiant source à partir duquel la règle gérée a été créée (`IAM_POLICY_IN_USE`).



Vous pouvez maintenant revenir à la console Audit Manager et sélectionner le même mot clé identifiant dans la liste déroulante.



Je souhaite partager un cadre personnalisé, mais il comporte des contrôles qui utilisent des règles AWS Config personnalisées comme source de données. Le destinataire peut-il collecter des preuves pour ces contrôles ?

Oui, le destinataire peut collecter des preuves pour ces contrôles, mais quelques étapes sont nécessaires pour y parvenir.

Pour qu'Audit Manager collecte des preuves en utilisant une règle AWS Config comme mappage de source de données, les conditions suivantes doivent être remplies. Cela s'applique aux règles gérées et aux règles personnalisées.

1. La règle doit exister dans l'environnement AWS du destinataire
2. La règle doit être activée dans l'environnement AWS du destinataire

N'oubliez pas que les règles AWS Config personnalisées de votre compte n'existent probablement pas encore dans l'environnement AWS du destinataire. De plus, lorsque le destinataire accepte la demande de partage, Audit Manager ne recrée aucune de vos règles personnalisées dans son compte. Pour que le destinataire puisse collecter des preuves en utilisant vos règles personnalisées comme mappage de source de données, il doit créer les mêmes règles personnalisées dans son instance de AWS Config. Une fois que le destinataire a créé puis activé les règles, Audit Manager peut collecter des preuves à partir de cette source de données.

Nous vous recommandons de communiquer avec le destinataire pour lui faire savoir si des règles personnalisées doivent être créées dans son instance de AWS Config.

Que se passe-t-il lorsqu'une règle personnalisée est mise à jour dans AWS Config ? Dois-je prendre des mesures dans Audit Manager ?

Pour les mises à jour des règles au sein de votre environnement AWS

Si vous mettez à jour une règle personnalisée dans votre environnement AWS, aucune action n'est nécessaire dans Audit Manager. Audit Manager détecte et gère les mises à jour des règles comme décrit dans le tableau suivant. Audit Manager ne vous avertit pas lorsqu'une mise à jour des règles est détectée.

Scénario	Ce que fait Audit Manager	Ce que vous devez faire
Une règle personnalisée est mise à jour dans votre instance de AWS Config.	Audit Manager continue de rapporter les résultats relatifs à cette règle à l'aide de la définition de règle mise à jour.	Aucune action n'est nécessaire.
Une règle personnalisée est supprimée de votre instance de AWS Config.	Audit Manager arrête de rapporter les résultats relatifs à la règle supprimée.	Aucune action n'est nécessaire. Si vous le souhaitez, vous pouvez modifier les contrôles personnalisés qui ont utilisé la règle supprimée comme mappage de source de données. Cela permet de nettoyer les paramètres de votre source de données en retirant la règle supprimée. Dans le cas contraire, le nom de la règle supprimée reste un mappage de source de données inutilisé.

Pour les mises à jour des règles en dehors de votre environnement AWS

Si une règle personnalisée est mise à jour en dehors de votre environnement AWS, Audit Manager ne détecte pas la mise à jour de la règle. C'est un élément à prendre en compte si vous utilisez des cadres personnalisés partagés. Cela est dû au fait que, dans ce scénario, l'expéditeur et le destinataire travaillent chacun dans des environnements AWS distincts. Le tableau suivant fournit les actions recommandées pour ce scénario.

Votre rôle	Scénario	Action recommandée
Expédi r	• Vous avez partagé un cadre qui utilise des règles personnalisées comme mappage de source de données. • Après avoir partagé le cadre, vous avez mis à jour ou supprimé l'une de ces règles dans AWS Config.	Informez le destinataire de votre mise à jour. Il peut ainsi appliquer la même mise à jour et rester synchronisé avec la dernière définition de règle.
Destina ire	• Vous avez accepté un cadre partagé qui utilise des règles personnalisées comme mappage de source de données. • Après avoir recréé les règles personnal isées dans votre instance de AWS Config, l'expéditeur a mis à jour ou supprimé l'une de ces règles.	Effectuez la mise à jour de la règle correspondante dans votre propre instance de AWS Config.

Résolution des problèmes liés au tableau de bord

Vous pouvez utiliser les informations de cette page pour résoudre les problèmes courants liés au tableau de bord dans Audit Manager.

Rubriques

- Mon tableau de bord ne comporte aucune donnée
- L'option de téléchargement CSV n'est pas disponible
- Je ne vois pas le fichier téléchargé lorsque j'essaie de télécharger un fichier CSV
- Un contrôle ou un domaine de contrôle spécifique est absent du tableau de bord
- L'instantané quotidien affiche des nombres variables de preuves tous les jours. Est-ce normal ?

Mon tableau de bord ne comporte aucune donnée

Si les chiffres du widget d'instantané quotidien sont marqués d'un trait d'union (-), cela indique qu'aucune donnée n'est disponible. Vous devez disposer d'au moins une évaluation active pour voir les données dans le tableau de bord. Pour commencer, créez une évaluation. Après une période de 24 heures, vos données d'évaluation commenceront à apparaître dans le tableau de bord.

> **Note**
>
> Si les chiffres du widget d'instantané quotidien affichent un zéro (0), cela indique que vos évaluations actives (ou l'évaluation que vous avez sélectionnée) ne contiennent aucune preuve non conforme.

L'option de téléchargement CSV n'est pas disponible

Cette option est disponible uniquement pour les évaluations individuelles. Assurez-vous d'avoir appliqué un the section called "Filtre d'évaluation" au tableau de bord, puis réessayez. N'oubliez pas que vous pouvez télécharger un seul fichier CSV à la fois.

Je ne vois pas le fichier téléchargé lorsque j'essaie de télécharger un fichier CSV

Si un domaine de contrôle contient un grand nombre de contrôles, il peut se produire un court délai avant que l'Audit Manager ne génère le fichier CSV. Une fois le fichier généré, celui-ci est automatiquement téléchargé.

Si le fichier téléchargé n'apparaît toujours pas, assurez-vous que votre connexion Internet fonctionne normalement et que vous utilisez la version la plus récente de votre navigateur Web. Vérifiez également votre dossier de téléchargements récents. Les fichiers sont téléchargés dans l'emplacement par défaut déterminé par votre navigateur. Si cela ne résout pas le problème, essayez de télécharger le fichier à l'aide d'un autre navigateur.

Un contrôle ou un domaine de contrôle spécifique est absent du tableau de bord

Cela signifie probablement que vos évaluations actives (ou l'évaluation spécifiée) ne contiennent aucune donnée pertinente pour ce contrôle ou ce domaine de contrôle.

Un domaine de contrôle est affiché sur le tableau de bord uniquement si les deux critères suivants sont remplis :

- Vos évaluations actives (ou l'évaluation spécifiée) contiennent au moins un contrôle lié à ce domaine
- Au moins un contrôle de ce domaine a collecté des preuves à la date indiquée en haut du tableau de bord

Un contrôle n'est affiché au sein d'un domaine que s'il a collecté des preuves à la date indiquée en haut du tableau de bord.

L'instantané quotidien affiche des nombres variables de preuves tous les jours. Est-ce normal ?

Les preuves ne sont pas toutes collectées quotidiennement. Les contrôles des évaluations d'Audit Manager sont mappés à différentes sources de données, et chacune d'elles peut avoir un calendrier de collecte de preuves différent. Par conséquent, il est prévu que l'instantané quotidien affiche un nombre variable de preuves tous les jours. Pour plus d'informations sur la fréquence de collecte des preuves, consultez How AWS Audit Manager collects evidence.

Résolution des problèmes liés aux administrateurs délégués et à AWS Organizations

Vous pouvez utiliser les informations de cette page pour résoudre les problèmes courants liés aux administrateurs délégués dans Audit Manager.

Rubriques

- Je ne parviens pas à configurer Audit Manager avec mon compte administrateur délégué
- Lorsque je crée une évaluation, je ne parviens pas à voir les comptes de mon organisation sous Comptes concernés
- Je reçois un message d'erreur accès refusé lorsque j'essaie de générer un rapport d'évaluation à l'aide de mon compte administrateur délégué
- Que se passe-t-il dans Audit Manager si je dissocie un compte membre de mon organisation ?
- Que se passe-t-il si je réassocie un compte membre à mon organisation ?
- Que se passe-t-il si je migre un compte membre d'une organisation vers une autre ?

Je ne parviens pas à configurer Audit Manager avec mon compte administrateur délégué

Bien que plusieurs administrateurs délégués soient pris en charge dans AWS Organizations, Audit Manager n'autorise qu'un seul administrateur délégué. Si vous essayez de désigner plusieurs administrateurs délégués dans Audit Manager, vous recevez le message d'erreur suivant :

- Console : `You have exceeded the allowed number of delegated administrators for the delegated service`
- CLI : `An error occurred (ValidationException) when calling the RegisterAccount operation: Cannot change delegated Admin for an active account 11111111111 from 2222222222222 to 333333333333`

Choisissez le compte individuel que vous souhaitez utiliser en tant qu'administrateur délégué dans Audit Manager. Assurez-vous d'abord d'enregistrer le compte administrateur délégué dans Organizations, puis d'ajouter le même compte en tant qu'administrateur délégué dans Audit Manager.

Lorsque je crée une évaluation, je ne parviens pas à voir les comptes de mon organisation sous Comptes concernés

Si vous souhaitez que votre évaluation Audit Manager inclue plusieurs comptes de votre organisation, vous devez spécifier un administrateur délégué.

Vérifiez que vous avez configuré un compte administrateur délégué pour Audit Manager. Pour obtenir des instructions, consultez Settings, Delegated administrator.

Voici quelques points à garder à l'esprit :

- Vous ne pouvez pas utiliser votre compte de gestion AWS Organizations en tant qu'administrateur délégué dans Audit Manager.
- Si vous souhaitez activer Audit Manager dans plusieurs Région AWS, vous devez désigner un compte d'administrateur délégué séparément dans chaque région. Dans vos paramètres Audit Manager, désignez le même compte administrateur délégué dans toutes les régions.
- Lorsque vous désignez un administrateur délégué, assurez-vous que le compte administrateur délégué a accès à la clé KMS que vous avez fournie lors de la configuration d'Audit Manager. Pour savoir comment vérifier et modifier vos paramètres de chiffrement, consultez Data encryption.

Je reçois un message d'erreur accès refusé lorsque j'essaie de générer un rapport d'évaluation à l'aide de mon compte administrateur délégué

Vous recevrez un message d'erreur `access denied` si votre évaluation a été créée par un compte administrateur délégué auquel la clé KMS spécifiée dans vos paramètres Audit Manager n'appartient pas. Pour éviter cette erreur, lorsque vous désignez un administrateur délégué pour Audit Manager, assurez-vous que le compte administrateur délégué a accès à la clé KMS que vous avez fournie lors de la configuration d'Audit Manager.

Vous pouvez également recevoir un message d'erreur `access denied` si vous ne disposez pas des autorisations d'écriture pour le compartiment S3 que vous utilisez comme destination de votre rapport d'évaluation.

Si vous recevez un message d'erreur `access denied`, veillez à respecter les exigences suivantes :

- Votre clé KMS dans vos paramètres Audit Manager donne des autorisations à l'administrateur délégué. Vous pouvez configurer ceci en suivant les instructions de la section Autoriser des utilisateurs d'autres comptes à utiliser une clé KMS dans le Guide du développeur d'AWS Key Management Service. Pour obtenir des instructions sur la vérification et la modification de vos paramètres de chiffrement dans Audit Manager, consultez Data encryption.
- Vous disposez d'une politique d'autorisation qui vous accorde un accès en écriture à la destination du rapport d'évaluation. Plus précisément, votre politique d'autorisation contient une action `s3:PutObject`, spécifie l'ARN du compartiment S3 et inclut la clé KMS utilisée pour chiffrer vos rapports d'évaluation. Pour un exemple de politique que vous pouvez utiliser, consultez Identity-based policy examples for AWS Audit Manager.

> **Note**
>
> Si vous modifiez vos paramètres de chiffrement des données dans Audit Manager, ces modifications s'appliqueront aux nouvelles évaluations que vous créerez à l'avenir. Cela inclut tous les rapports d'évaluation que vous créez à partir de vos nouvelles évaluations.
> Les modifications ne s'appliquent pas aux évaluations existantes que vous avez créées avant de modifier vos paramètres de chiffrement. Cela inclut les nouveaux rapports d'évaluation que vous créez à partir d'évaluations existantes, en plus des rapports d'évaluation existants.
> Les évaluations existantes, ainsi que tous leurs rapports d'évaluation, continuent d'utiliser l'ancienne clé KMS. Si l'identité IAM qui génère le rapport d'évaluation n'est pas autorisée à

utiliser l'ancienne clé KMS, vous pouvez accorder des autorisations au niveau de la stratégie de clé.

Que se passe-t-il dans Audit Manager si je dissocie un compte membre de mon organisation ?

Lorsque vous dissociez un compte membre d'une organisation, Audit Manager reçoit une notification concernant cet événement. Audit Manager supprime ensuite automatiquement cet Compte AWS des listes des comptes concernés par vos évaluations existantes. Lorsque vous définissez l'étendue des nouvelles évaluations à venir, le compte dissocié n'apparaît plus dans la liste des Comptes AWS éligibles.

Lorsqu'Audit Manager supprime un compte membre dissocié des listes des comptes concernés par vos évaluations, vous n'êtes pas informé de cette modification. De plus, le compte membre dissocié n'est pas informé qu'Audit Manager n'est plus activé sur son compte.

Que se passe-t-il si je réassocie un compte membre à mon organisation ?

Lorsque vous réassociez un compte membre à votre organisation, ce compte n'est pas automatiquement ajouté à l'étendue de vos évaluations Audit Manager existantes. Toutefois, le compte membre réassocié apparaît désormais comme Compte AWS éligible lorsque vous spécifiez les comptes concernés par vos évaluations.

- Pour les évaluations existantes, vous pouvez modifier manuellement l'étendue de l'évaluation pour ajouter le compte membre réassocié. Pour obtenir des instructions, consultez Edit Comptes AWS in scope.
- Pour les nouvelles évaluations, vous pouvez ajouter le compte réassocié lors de la configuration de l'évaluation. Pour obtenir des instructions, consultez Specify Comptes AWS in scope.

Que se passe-t-il si je migre un compte membre d'une organisation vers une autre ?

Si Audit Manager est activé sur un compte membre dans l'organisation 1, mais que ce compte migre vers l'organisation 2, Audit Manager n'est pas activé pour l'organisation 2.

Résolution des problèmes liés à l'outil de recherche de preuves

Utilisez les informations de cette page pour résoudre les problèmes courants liés à l'outil de recherche de preuves dans Audit Manager.

Problèmes généraux liés à l'outil de recherche de preuves

- Je ne parviens pas à activer l'outil de recherche de preuves
- J'ai activé l'outil de recherche de preuves, mais je ne vois pas les preuves passées dans mes résultats de recherche
- Je ne parviens pas à désactiver l'outil de recherche de preuves
- Ma requête de recherche échoue

Problèmes liés aux rapports d'évaluation dans l'outil de recherche de preuves

- Je ne parviens pas à générer plusieurs rapports d'évaluation à partir des résultats de ma recherche
- Je ne parviens pas à inclure des preuves spécifiques à partir des résultats de ma recherche
- Les résultats de ma recherche de preuves ne sont pas tous inclus dans le rapport d'évaluation
- Je souhaite générer un rapport d'évaluation à partir des résultats de ma recherche, mais mon instruction de requête échoue
- Ressources supplémentaires

Problèmes d'exportation au format CSV dans l'outil de recherche de preuves

- Mon exportation au format CSV a échoué
- Je ne parviens pas à exporter des preuves spécifiques à partir des résultats de ma recherche
- Je ne peux pas exporter plusieurs fichiers CSV à la fois

Je ne parviens pas à activer l'outil de recherche de preuves

Les raisons courantes pour lesquelles vous ne pouvez pas activer l'outil de recherche de preuves sont les suivantes :

Il vous manque des autorisations

Si vous essayez d'activer l'outil de recherche de preuves pour la première fois, assurez-vous de disposer des autorisations requises. Ces autorisations vous permettent de créer et de gérer un magasin de données d'événements dans CloudTrail Lake, ce qui est nécessaire pour prendre en charge les requêtes de recherche de l'outil de recherche de preuves. Les autorisations vous permettent également d'exécuter des requêtes de recherche dans l'outil de recherche de preuves.

Si vous avez besoin d'aide concernant les autorisations, contactez votre administrateur AWS. Si vous êtes un administrateur AWS, vous pouvez copier la déclaration d'autorisation requise et la joindre à une politique IAM.

Vous utilisez votre compte de gestion Organizations

N'oubliez pas que vous pouvez utiliser votre compte de gestion pour activer l'outil de recherche de preuves. Connectez-vous en tant que compte administrateur délégué, puis réessayez.

Vous avez précédemment désactivé l'outil de recherche de preuves

La réactivation de l'outil de recherche de preuves n'est actuellement pas prise en charge. Si vous avez précédemment désactivé l'outil de recherche de preuves, vous ne pourrez pas l'activer à nouveau.

J'ai activé l'outil de recherche de preuves, mais je ne vois pas les preuves passées dans mes résultats de recherche

Lorsque vous activez l'outil de recherche de preuves, il faut jusqu'à 7 jours pour que toutes vos données de preuves passées soient disponibles.

Au cours de cette période de 7 jours, un magasin de données d'événements est rempli avec vos données de preuves des deux dernières années. Cela signifie que si vous utilisez l'outil de recherche de preuves immédiatement après l'avoir activé, tous les résultats ne seront pas disponibles tant que le remplissage ne sera pas terminé.

Pour obtenir des instructions sur la façon de vérifier le statut du remplissage des données, consultez Confirming the status of evidence finder.

Je ne parviens pas à désactiver l'outil de recherche de preuves

Cela peut être dû à l'une des raisons suivantes.

Il vous manque des autorisations

Si vous essayez de désactiver l'outil de recherche de preuves, assurez-vous que vous disposez des autorisations requises. Ces autorisations vous permettent de mettre à jour et de supprimer un magasin de données d'événements dans CloudTrail Lake, ce qui est nécessaire pour désactiver l'outil de recherche de preuves.

Si vous avez besoin d'aide concernant les autorisations, contactez votre administrateur AWS. Si vous êtes un administrateur AWS, vous pouvez copier la déclaration d'autorisation requise et la joindre à une politique IAM.

Une demande visant à activer l'outil de recherche de preuves est toujours en cours

Lorsque vous demandez d'activer l'outil de recherche de preuves, nous créons un magasin de données d'événements pour répondre aux requêtes de l'outil de recherche de preuves. Vous ne pouvez pas désactiver l'outil de recherche de preuves lors de la création du magasin de données d'événements.

Pour continuer, attendez que le magasin de données d'événements soit créé, puis réessayez. Pour plus d'informations, consultez Confirming the status of evidence finder.

Vous avez déjà demandé de désactiver l'outil de recherche de preuves

Lorsque vous demandez de désactiver l'outil de recherche de preuves, nous supprimons le magasin de données d'événements utilisé pour les requêtes de l'outil de recherche de preuves. Si vous essayez à nouveau de désactiver l'outil de recherche de preuves alors que le magasin de données d'événements est supprimé, un message d'erreur s'affiche.

Dans ce cas, aucune action n'est nécessaire. Attendez que le magasin de données d'événements soit supprimé. Dès que cette opération est terminée, l'outil de recherche de preuves est désactivé. Pour plus d'informations, consultez Confirming the status of evidence finder.

Ma requête de recherche échoue

L'échec d'une requête de recherche peut être dû à l'une des raisons suivantes.

Il vous manque des autorisations

Vérifiez que l'utilisateur dispose des autorisations requises pour exécuter des requêtes de recherche et accéder aux résultats de recherche. Plus précisément, vous avez besoin d'autorisations pour les actions CloudTrail suivantes :

- StartQuery
- DescribeQuery
- CancelQuery
- GetQueryResults

Si vous avez besoin d'aide concernant les autorisations, contactez votre administrateur AWS. Si vous êtes un administrateur AWS, vous pouvez copier la déclaration d'autorisation requise et la joindre à une politique IAM.

Vous exécutez le nombre maximal de requêtes

Vous pouvez exécuter jusqu'à 5 requêtes à la fois. Si vous exécutez le nombre maximal de requêtes simultanées, cela entraîne une erreur `MaxConcurrentQueriesException`. Si ce message d'erreur s'affiche, attendez une minute que certaines requêtes soient terminées, puis réexécutez la requête.

Votre instruction de requête contient une erreur de validation

Si vous utilisez l'API ou la CLI pour effectuer l'opération StartQuery de CloudTrail Lake, assurez-vous que votre `queryStatement` est valide. Si l'instruction de requête comporte des erreurs de validation, une syntaxe incorrecte ou des mots clés non pris en charge, cela se traduit par une `InvalidQueryStatementException`.

Pour plus d'informations sur l'écriture d'une requête, consultez Créer ou modifier une requête dans le Guide de l'utilisateur d'AWS CloudTrail.

Pour obtenir des exemples de syntaxe valide, consultez les exemples d'instructions de requêtes suivants qui peuvent être utilisés pour interroger un magasin de données d'événements dans Audit Manager.

Exemple 1 : Examiner les preuves et leur statut de conformité

Cet exemple permet de rechercher des preuves, quel que soit leur statut de conformité, dans toutes les évaluations prises en compte, dans une plage de dates spécifiée.

```
SELECT eventData.evidenceId, eventData.resourceArn,
 eventData.resourceComplianceCheck FROM $EDS_ID WHERE eventTime > '2022-11-02
 00:00:00.000' AND eventTime < '2022-11-03 00:00:00.000'
```

Exemple 2 : Déterminer les preuves non conformes d'un contrôle

Cet exemple permet de rechercher toutes les preuves non conformes dans une plage de dates spécifiée pour une évaluation et un contrôle spécifiques.

```
SELECT * FROM $EDS_ID WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-
ff22gg44hh66' AND eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.resourceComplianceCheck IN
 ('NON_COMPLIANT','FAILED','WARNING') AND eventData.controlId IN ('aa11bb22-cc33-
dd44-ee55-ff66gg77hh88')
```

Exemple 3 : Compter les preuves par nom

Cet exemple répertorie le nombre total de preuves d'une évaluation dans une plage de dates spécifiée, groupées par nom et classées par nombre de preuves.

```
SELECT eventData.eventName as eventName, COUNT(*) as totalEvidence FROM  $EDS_ID
 WHERE eventData.assessmentId = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime
 > '2022-10-27 22:05:00.000' AND eventTime < '2022-11-03 22:05:00.000' GROUP BY
 eventData.eventName ORDER BY totalEvidence DESC
```

Exemple 4 : Explorer les preuves par source de données et par service

Cet exemple permet de rechercher toutes les preuves dans une plage de dates spécifiée pour une source de données et un service spécifiques.

```
SELECT * FROM $EDS_ID WHERE eventTime > '2022-10-27 22:05:00.000' AND eventTime
 < '2022-11-03 22:05:00.000' AND eventData.service IN ('dynamodb') AND
 eventData.dataSource IN ('AWS API calls')
```

Exemple 5 : Explorer les preuves conformes par source de données et domaine de contrôle

Cet exemple permet de rechercher des preuves conformes pour des domaines de contrôle spécifiques, lorsque les preuves proviennent d'une source de données autre qu'AWS Config.

```
 SELECT * FROM $EDS_ID WHERE eventData.resourceComplianceCheck IN
 ('PASSED','COMPLIANT') AND eventData.controlDomainName IN ('Logging and
 monitoring','Data security and privacy') AND eventData.dataSource NOT IN ('AWS
 Config')
```

Autres exceptions d'API

L'API StartQuery peut échouer pour plusieurs autres raisons. Pour obtenir la liste complète des erreurs possibles et leur description, consultez StartQuery Errors dans laAWS CloudTrail Référence de l'API.

Je ne parviens pas à générer plusieurs rapports d'évaluation à partir des résultats de ma recherche

Cette erreur est due à l'exécution simultanée d'un trop grand nombre de requêtes CloudTrail Lake.

Cette erreur peut se produire si vous regroupez les résultats de votre recherche et tentez de générer immédiatement des rapports d'évaluation pour chaque élément de ligne de vos résultats regroupés. Lorsque vous obtenez les résultats de votre recherche et que vous générez un rapport d'évaluation, chaque action invoque une requête. Vous ne pouvez exécuter que 5 requêtes à la fois. Si vous exécutez le nombre maximal de requêtes simultanées, l'erreur `MaxConcurrentQueriesException` est renvoyée.

Pour éviter cette erreur, assurez-vous de ne pas générer trop de rapports d'évaluation à la fois. Si vous exécutez le nombre maximal de requêtes simultanées, l'erreur `MaxConcurrentQueriesException` est renvoyée. Si ce message d'erreur s'affiche, attendez quelques minutes que vos rapports d'évaluation en cours soient terminés.

Vous pouvez vérifier le statut de vos rapports d'évaluation depuis la page du centre de téléchargement de la console Audit Manager. Une fois vos rapports terminés, revenez à vos résultats regroupés dans l'outil de recherche de preuves. Vous pouvez ensuite continuer à obtenir les résultats et à générer un rapport d'évaluation pour chaque élément de ligne.

Je ne parviens pas à inclure des preuves spécifiques à partir des résultats de ma recherche

Tous les résultats de votre recherche sont inclus dans le rapport d'évaluation. Vous ne pouvez pas ajouter de lignes individuelles de manière sélective à partir de votre ensemble de résultats de recherche.

Si vous souhaitez uniquement inclure des résultats de recherche spécifiques dans le rapport d'évaluation, nous vous recommandons de modifier vos filtres de recherche actuels. Ainsi, vous

pouvez affiner vos résultats pour cibler uniquement les preuves que vous souhaitez inclure dans le rapport.

Les résultats de ma recherche de preuves ne sont pas tous inclus dans le rapport d'évaluation

Lorsque vous générez un rapport d'évaluation, le nombre de preuves que vous pouvez ajouter est limité. La limite dépend de l'Région AWS de votre évaluation, de la région du compartiment S3 utilisé comme destination de votre rapport d'évaluation et du fait que votre évaluation utilise ou non une AWS KMS key gérée par le client.

1. La limite est de 22 000 pour les rapports d'une même région (dans le cas où le compartiment S3 et l'évaluation se trouvent dans la même Région AWS)
2. La limite est de 3 500 pour les rapports interrégionaux (dans le cas où le compartiment S3 et l'évaluation se trouvent dans des Régions AWS différentes)
3. La limite est de 3 500 si l'évaluation utilise une clé KMS gérée par le client

Si vous dépassez cette limite, le rapport est quand même créé. Toutefois, Audit Manager ajoute uniquement les 3 500 ou 22 000 premiers éléments de preuves au rapport.

Pour éviter ce problème, nous vous recommandons de modifier vos filtres de recherche actuels. De cette façon, vous pouvez réduire les résultats de votre recherche en ciblant un plus petit nombre de preuves. Si nécessaire, vous pouvez répéter cette méthode et générer plusieurs rapports d'évaluation au lieu d'un seul rapport plus volumineux.

Je souhaite générer un rapport d'évaluation à partir des résultats de ma recherche, mais mon instruction de requête échoue

Si vous utilisez l'API CreateAssessmentReport et que votre instruction de requête renvoie une exception de validation, consultez le tableau ci-dessous pour savoir comment y remédier.

> **Note**
>
> Même si une instruction de requête fonctionne dans CloudTrail, il est possible que la même requête ne soit pas valide pour la génération du rapport d'évaluation dans Audit Manager. Cela est dû à certaines différences dans la validation des requêtes entre les deux services.

Clause	Problème	Solution	Remarques
`SELECT`	La clause `SELECT` contient un nom de colonne	Supprimez la clause `SELECT` et remplacez-la par `SELECT eventJson` .	Seule la clause `SELECT eventJson` est prise en charge. Cette validation est gérée par Audit Manager.
`FROM`	La clause `FROM` contient un identifiant de magasin de données d'événements non valide ou L'identifiant de magasin de données d'événements fourni ne correspond pas à l'identifiant de magasin de données d'événements dans vos paramètres Audit Manager	Supprimez la clause `FROM` et remplacez-la par `FROM edsID`, où la valeur de `edsID` correspond à l'ID de magasin de données d'événements spécifié dans vos paramètres Audit Manager. Vous pouvez récupérer l'ARN du magasin de données d'événements à partir de vos paramètres Audit Manager. Pour plus d'informations, consultez GetSettings dans laAWS Audit Manager Référence de l'API.	Cette validation est gérée par Audit Manager.
`GROUP BY`	La clause `GROUP BY` est présente dans la requête	Supprimez la clause `GROUP BY`.	Cette validation est gérée par Audit Manager.
`HAVING`	La clause `HAVING` est présente dans la requête	Supprimez la clause `HAVING`.	Cette validation est gérée par Audit Manager.
`LIMIT`	La clause `LIMIT` contient une valeur	Si la clause `LIMIT` existe, assurez-vous que sa valeur est	Dans la console, il n'y a aucune limite au nombre de résultats de preuves pouvant

Clause	Problème	Solution	Remarques
	qui dépasse la limite maximale autorisée	égale ou inférieure à la limite maximale prise en charge : • Pour les rapports d'une même région, la limite est de 22 000 • Pour les rapports interrégionaux, la limite est de 3 500 • Pour les rapports où l'évaluation associée utilise une AWS KMS key gérée par le client, la limite est de 3 500	être renvoyés. Toutefois, lors de la génération d'un rapport d'évaluation, une limite s'applique au nombre de preuves que vous pouvez inclure. Si aucune valeur `LIMIT` n'est fournie dans votre instruction de requête, les limites maximales par défaut sont appliquées. Cette validation est gérée par Audit Manager.
`ORDER BY`	La clause `ORDER BY` contient des fonctions d'agrégation ou des alias qui ne sont pas présents dans la clause `SELECT`	Assurez-vous que la clause `ORDER BY` ne contient aucune condition utilisant des fonctions d'agrégation ou des alias.	Cette validation est gérée par l'API StartQuery de CloudTrail.

Clause	Problème	Solution	Remarques
`WHERE`	La clause `WHERE` contient plusieurs `assessmentId` ou La clause `WHERE` contient un `assessmentId` qui ne correspond pas à l'`assessmentId` de votre demande `createAssessmentReport` ou La clause `WHERE` contient un nom de colonne non pris en charge	Assurez-vous qu'un seul assessmentID est spécifié et qu'il correspond au paramètre assessmentID que vous avez spécifié dans la demande d'API `createAssessmentReport` . Supprimez tous les noms de colonnes non pris en charge.	Cette validation est gérée par l'API StartQuery de CloudTrail.

Exemples

Les exemples suivants montrent comment utiliser le paramètre `queryStatement` lorsque vous appelez l'opération CreateAssessmentReport. Avant d'utiliser ces requêtes, remplacez le *`texte de l'espace réservé`* par vos propres valeurs `edsId` et `assessmentId`.

Exemple 1 : Créer un rapport (la limite de même région s'applique)

Cet exemple crée un rapport qui inclut les résultats des compartiments S3 créés entre le 22 et le 23 janvier 2022.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' AND eventTime > '2022-01-22 00:00:00.000' AND
 eventTime < '2022-01-23 00:00:00.000' AND eventName='CreateBucket' LIMIT 22000
```

Exemple 2 : Créer un rapport (la limite interrégionale s'applique)

Cet exemple crée un rapport qui inclut tous les résultats du magasin de données d'événements et de l'évaluation spécifiés, sans qu'aucune plage de dates soit spécifiée.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 7000
```

Exemple 3 : Créer un rapport (sous la limite par défaut)

Cet exemple crée un rapport qui inclut tous les résultats du magasin de données d'événements et de l'évaluation spécifiés, avec une limite inférieure au maximum par défaut.

```
SELECT eventJson FROM 12345678-abcd-1234-abcd-123456789012 WHERE eventData.assessmentId
 = '11aa33bb-55cc-77dd-99ee-ff22gg44hh66' LIMIT 2000
```

Ressources supplémentaires

La page suivante contient des conseils généraux pour la résolution des problèmes liés aux rapports d'évaluation :

- Résolution des problèmes liés aux rapports d'évaluation

Mon exportation au format CSV a échoué

Votre exportation au format CSV peut échouer pour plusieurs raisons. Vous pouvez résoudre ce problème en vérifiant les causes les plus fréquentes.

Tout d'abord, vérifiez que vous remplissez les conditions requises pour utiliser la fonctionnalité d'exportation au format CSV :

Vous avez activé l'outil de recherche de preuves avec succès

Si vous n'avez pas activé l'outil de recherche de preuves, vous ne pouvez pas exécuter de requête de recherche et exporter les résultats de votre recherche.

Le remplissage de votre magasin de données d'événements est terminé

Si vous utilisez l'outil de recherche de preuves immédiatement après l'avoir activé et que le remplissage des preuves est toujours en cours, il se peut que certains résultats ne soient pas disponibles. Pour vérifier le statut du remplissage, consultez Confirm the status of evidence finder.

Votre requête de recherche a réussi

> Audit Manager ne peut pas exporter les résultats d'une requête ayant échoué. Pour résoudre les problèmes liés à l'échec d'une requête, consultez Ma requête de recherche échoue.

Après avoir vérifié que vous remplissez les conditions requises, utilisez la liste de contrôle suivante pour vérifier les problèmes potentiels :

1. Vérifiez le statut de votre requête de recherche :
   a. La requête a-t-elle été annulée ? L'outil de recherche de preuves affiche des résultats partiels traités avant l'annulation de la requête. Toutefois, Audit Manager n'exporte pas les résultats partiels vers votre compartiment S3 ou le centre de téléchargement.
   b. La requête est-elle en cours d'exécution depuis plus d'une heure ? Les requêtes qui s'exécutent pendant plus d'une heure peuvent prendre fin. L'outil de recherche de preuves affiche des résultats partiels traités avant l'expiration de la requête. Toutefois, Audit Manager n'exporte pas de résultats partiels. Pour éviter un dépassement de délai, vous pouvez réduire le nombre de preuves analysées en modifiant votre requête de recherche pour spécifier une plage de temps plus étroite.
2. Vérifiez le nom et l'URI du compartiment S3 de destination de votre exportation :
   a. Le compartiment que vous avez spécifié existe-t-il ? Si vous avez saisi manuellement l'URI d'un compartiment, assurez-vous de ne pas avoir commis d'erreur de frappe. Une faute de frappe ou un URI incorrect peut générer une erreur `RESOURCE_NOT_FOUND` lorsqu'Audit Manager tente d'exporter le fichier CSV vers Amazon S3.
3. Vérifiez les autorisations du compartiment S3 de destination de votre exportation :
   a. Disposez-vous d'autorisations d'écriture pour le compartiment S3 ? Vous devez disposer d'un accès en écriture pour le compartiment S3 que vous utilisez comme destination d'exportation. Plus précisément, la politique d'autorisation IAM doit inclure une action `s3:PutObject` et l'ARN du compartiment, et répertorier CloudTrail comme principal de service. Nous fournissons un exemple de politique que vous pouvez utiliser. Pour obtenir des instructions sur l'utilisation d'un compartiment S3 différent, consultez Export destination settings.
4. Vérifiez si certaines de vos informations en matière d'Région AWS ne concordent pas :
   a. L'Région AWS de la clé gérée par votre client correspond-elle à l'Région AWS de votre évaluation ? Si vous avez fourni une clé gérée par le client pour le chiffrement des données, celle-ci doit se trouver dans la même Région AWS que celle de votre évaluation. Pour obtenir des instructions sur la modification de la clé KMS, consultez Chiffrement des données.

5. Vérifiez les autorisations de votre compte administrateur délégué :
   a. La clé gérée par le client dans vos paramètres Audit Manager accorde-t-elle des autorisations à votre administrateur délégué ? Si vous utilisez un compte administrateur délégué et que vous avez spécifié une clé gérée par le client pour le chiffrement des données, assurez-vous que l'administrateur délégué a accès à cette clé KMS. Pour obtenir des instructions, consultez Autoriser des utilisateurs d'autres comptes à utiliser une clé KMS dans le Guide du développeur d'AWS Key Management Service. Pour vérifier et modifier vos paramètres de chiffrement dans Audit Manager, consultez Data encryption settings.

> **Note**
>
> Si vous modifiez vos paramètres de chiffrement des données Audit Manager, ces modifications s'appliqueront aux nouvelles évaluations que vous créerez à l'avenir. Cela inclut tous les fichiers CSV que vous exportez à partir de vos nouvelles évaluations.
> Les modifications ne s'appliquent pas aux évaluations existantes que vous avez créées avant de modifier vos paramètres de chiffrement. Cela inclut les nouvelles exportations au format CSV à partir d'évaluations existantes, en plus des exportations au format CSV existantes. Les évaluations existantes, ainsi que toutes leurs exportations au format CSV, continuent d'utiliser l'ancienne clé KMS. Si l'identité IAM qui exporte le fichier CSV n'est pas autorisée à utiliser l'ancienne clé KMS, vous pouvez accorder des autorisations au niveau de la stratégie de clé.

Je ne parviens pas à exporter des preuves spécifiques à partir des résultats de ma recherche

Tous les résultats de votre recherche sont inclus dans les résultats.

Si vous souhaitez inclure uniquement des preuves spécifiques dans le fichier CSV, nous vous recommandons de modifier vos filtres de recherche actuels. Ainsi, vous pouvez affiner vos résultats pour cibler uniquement les preuves que vous souhaitez exporter.

Je ne peux pas exporter plusieurs fichiers CSV à la fois

Cette erreur est due à l'exécution simultanée d'un trop grand nombre de requêtes CloudTrail Lake.

Cela peut se produire si vous regroupez les résultats de votre recherche et tentez d'exporter immédiatement un fichier CSV pour chaque élément de ligne de vos résultats regroupés. Lorsque

vous obtenez les résultats de votre recherche et que vous exportez un fichier CSV, chacune de ces actions invoque une requête. Vous ne pouvez exécuter que cinq requêtes à la fois. Si vous exécutez le nombre maximal de requêtes simultanées, l'erreur `MaxConcurrentQueriesException` est renvoyée.

Pour éviter cette erreur, assurez-vous de ne pas exporter trop de fichiers CSV à la fois.

Pour résoudre cette erreur, attendez que vos exportations au format CSV en cours soient terminées. La plupart des exportations prennent quelques minutes. Toutefois, si vous exportez une très grande quantité de données, l'exportation peut prendre jusqu'à une heure. N'hésitez pas à quitter l'outil de recherche de preuves pendant que l'exportation est en cours.

Vous pouvez vérifier le statut de l'exportation depuis le centre de téléchargement de la console Audit Manager. Une fois que vos fichiers exportés sont prêts, revenez à vos résultats regroupés dans l'outil de recherche de preuves. Vous pouvez ensuite continuer à obtenir les résultats et à exporter un fichier CSV pour chaque élément de ligne.

Résolution des problèmes liés au partage de cadre

Vous pouvez utiliser les informations de cette page pour résoudre les problèmes courants liés au partage de cadre dans Audit Manager.

Rubriques

- Le statut de ma demande de partage envoyée s'affiche comme Échec
- Ma demande de partage est accompagnée d'un point bleu. Qu'est-ce que cela signifie ?
- Mon cadre partagé comporte des contrôles qui utilisent des règles AWS Config personnalisées comme source de données. Le destinataire peut-il collecter des preuves pour ces contrôles ?
- J'ai mis à jour une règle personnalisée utilisée dans un cadre partagé. Dois-je prendre des mesures ?

Le statut de ma demande de partage envoyée s'affiche comme Échec

Si vous essayez de partager un cadre personnalisé et que l'opération échoue, nous vous recommandons de vérifier les points suivants :

1. Assurez-vous qu'Audit Manager est activé dans le Compte AWS du destinataire et dans la région spécifiée. Pour la liste des régions AWS Audit Manager prises en charge, consultez AWS Audit Manager endpoints and quotas dans le document Référence générale d'Amazon Web Services.

2. Assurez-vous d'avoir saisi l'identifiant du bon Compte AWS lorsque vous avez spécifié le compte du destinataire.
3. Assurez-vous de ne pas avoir spécifié de compte de gestion AWS Organizations comme destinataire. Vous pouvez partager un cadre personnalisé avec un administrateur délégué, mais si vous essayez de partager un cadre personnalisé avec un compte de gestion, l'opération échoue.
4. Si vous utilisez une clé gérée par le client pour chiffrer vos données Audit Manager, assurez-vous que votre clé KMS est activée. Si votre clé KMS est désactivée et que vous essayez de partager un cadre personnalisé, l'opération échoue. Pour obtenir des instructions sur l'activation d'une clé KMS désactivée, consultez Activation et désactivation des clés dans le Guide du développeur d'AWS Key Management Service.

Ma demande de partage est accompagnée d'un point bleu. Qu'est-ce que cela signifie ?

Une notification à point bleu indique qu'une demande de partage nécessite votre attention.

Notifications à point bleu destinées aux expéditeurs

Un point de notification bleu apparaît à côté des demandes de partage envoyées dont le statut est Expiration. Audit Manager affiche la notification à point bleu afin que vous puissiez rappeler au destinataire de donner suite à la demande de partage avant son expiration.

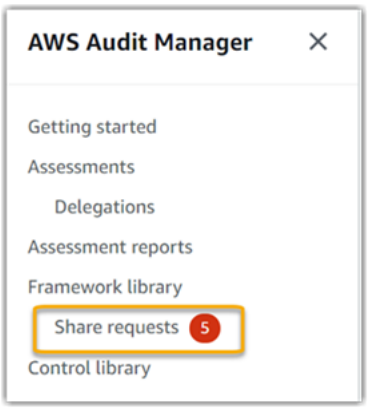
Pour que le point bleu de notification disparaisse, le destinataire doit accepter ou refuser la demande. Le point bleu disparaît également si vous révoquez la demande de partage.

Vous pouvez utiliser la procédure suivante pour vérifier si des demandes de partage arrivent à expiration et envoyer un rappel facultatif au destinataire pour qu'il prenne les mesures nécessaires.

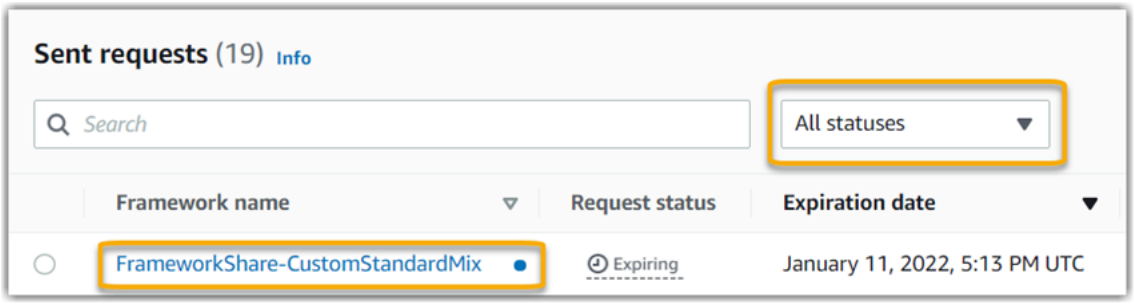
Pour afficher les notifications relatives aux demandes envoyées

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Si vous avez reçu une notification de demande de partage, Audit Manager affiche un point rouge à côté de l'icône du menu de navigation.

3. Développez le volet de navigation et regardez à côté de Demandes de partage. Un badge de notification indique le nombre de demandes de partage nécessitant une attention particulière.



4. Choisissez Demandes de partage, puis sélectionnez l'onglet Demandes envoyées.
5. Recherchez le point bleu pour identifier les demandes de partage qui expireront dans les 30 prochains jours. Vous pouvez également consulter les demandes de partage arrivant à expiration en sélectionnant Expiration dans le menu déroulant du filtre Tous les statuts.



6. (Facultatif) Rappelez au destinataire qu'il doit donner suite à la demande de partage avant son expiration. Cette étape est facultative, car Audit Manager envoie une notification dans la console pour informer le destinataire lorsqu'une demande de partage est active ou expire. Cependant, vous pouvez également envoyer votre propre rappel au destinataire en utilisant votre canal de communication préféré.

Notifications à point bleu destinées aux destinataires

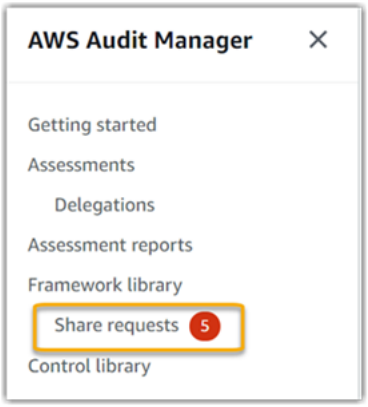
Un point bleu de notification apparaît à côté des demandes de partage reçues dont le statut est Actif ou Expiration. Audit Manager affiche la notification à point bleu pour vous rappeler de donner suite à la demande de partage avant son expiration. Pour que le point de notification bleu disparaisse, vous devez accepter ou refuser la demande. Le point bleu disparaît également si l'expéditeur révoque la demande de partage.

Vous pouvez utiliser la procédure suivante pour vérifier les demandes de partage actives et en cours d'expiration.

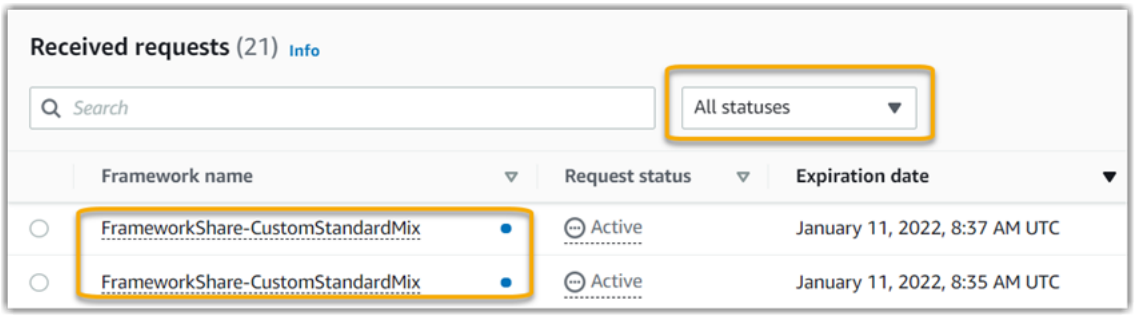
Pour afficher les notifications relatives aux demandes reçues

1. Ouvrez la console AWS Audit Manager à l'adresse https://console.aws.amazon.com/auditmanager/home.
2. Si vous avez reçu une notification de demande de partage, Audit Manager affiche un point rouge à côté de l'icône du menu de navigation.

3. Développez le volet de navigation et regardez à côté de Demandes de partage. Un badge de notification indique le nombre de demandes de partage qui nécessitent votre attention.



4. Choisissez Demandes de partage. Par défaut, cette page s'ouvre dans l'onglet Demandes reçues.
5. Identifiez les demandes de partage qui nécessitent une action de votre part en recherchant les éléments marqués d'un point bleu.



6. (Facultatif) Pour afficher uniquement les demandes qui expireront dans les 30 prochains jours, recherchez la liste déroulante Tous les statuts et sélectionnez Arrive à expiration.

Mon cadre partagé comporte des contrôles qui utilisent des règles AWS Config personnalisées comme source de données. Le destinataire peut-il collecter des preuves pour ces contrôles ?

Oui, votre destinataire peut collecter des preuves pour ces contrôles, mais quelques étapes sont nécessaires pour y parvenir.

Pour qu'Audit Manager collecte des preuves en utilisant une règle AWS Config comme mappage de source de données, les conditions suivantes doivent être remplies. Ces critères s'appliquent à la fois aux règles gérées et aux règles personnalisées.

- La règle doit exister dans l'environnement AWS du destinataire.
- La règle doit être activée dans l'environnement AWS du destinataire.

N'oubliez pas que les règles AWS Config de votre compte n'existent probablement pas déjà dans l'environnement AWS du destinataire. De plus, lorsque le destinataire accepte la demande de partage, Audit Manager ne recrée aucune de vos règles personnalisées dans son compte. Pour que le destinataire puisse collecter des preuves en utilisant vos règles personnalisées comme mappage de source de données, il doit créer les mêmes règles personnalisées dans son instance de AWS Config. Une fois que le destinataire a créé puis activé les règles dans AWS Config, Audit Manager peut collecter des preuves à partir de cette source de données.

Nous vous recommandons de communiquer avec le destinataire pour lui faire savoir si des règles AWS Config personnalisées doivent être créées dans son instance de AWS Config.

J'ai mis à jour une règle personnalisée utilisée dans un cadre partagé. Dois-je prendre des mesures ?

Pour les mises à jour des règles au sein de votre environnement AWS

Lorsque vous mettez à jour une règle personnalisée dans votre environnement AWS, aucune action n'est nécessaire dans Audit Manager. Audit Manager détecte et gère les mises à jour des règles de la manière décrite dans le tableau suivant. Audit Manager ne vous avertit pas lorsqu'une mise à jour des règles est détectée.

Scénario	Ce que fait Audit Manager	Ce que vous devez faire
Une règle personnalisée est mise à jour dans votre instance de AWS Config.	Audit Manager continue de rapporter les résultats relatifs à cette règle à l'aide de la définition de règle mise à jour.	Aucune action n'est nécessaire.
Une règle personnalisée est supprimée de votre instance de AWS Config.	Audit Manager arrête de rapporter les résultats relatifs à la règle supprimée.	Aucune action n'est nécessaire. Si vous le souhaitez, vous pouvez modifier les contrôles personnalisés qui ont utilisé la règle supprimée comme mappage de source de données. Vous pouvez ensuite retirer la règle supprimée pour nettoyer les paramètres de source de données de votre contrôle. Dans le cas contraire, le nom de la règle supprimée reste un mappage de source de données inutilisé.

Pour les mises à jour des règles en dehors de votre environnement AWS

Dans l'environnement AWS du destinataire, Audit Manager ne détecte pas la mise à jour des règles. Cela est dû au fait que les expéditeurs et les destinataires travaillent chacun dans des environnements AWS distincts. Le tableau suivant fournit les actions recommandées pour ce scénario.

Votre rôle	Scénario	Action recommandée
Expédi r	• Vous avez partagé un cadre qui utilise des règles personnalisées comme mappage de source de données.	Contactez le destinataire pour l'informe r de la mise à jour. Il peut ainsi effectuer

Votre rôle	Scénario	Action recommandée
	• Après avoir partagé le cadre, vous avez mis à jour ou supprimé l'une de ces règles dans AWS Config.	la même mise à jour et rester synchronisé avec la dernière définition de règle.
Destinataire	• Vous avez accepté un cadre partagé qui utilise des règles personnalisées comme mappage de source de données. • Après avoir recréé les règles personnalisées dans votre instance de AWS Config, l'expéditeur a mis à jour ou supprimé l'une de ces règles.	Effectuez la mise à jour de la règle correspondante dans votre propre instance de AWS Config.

Résolution des problèmes liés aux notifications

Vous pouvez utiliser les informations de cette page pour résoudre les problèmes courants de notification dans Audit Manager.

Rubriques

- J'ai spécifié une rubrique Amazon SNS dans Audit Manager, mais je ne reçois aucune notification
- J'ai spécifié une rubrique FIFO, mais je ne reçois pas de notifications dans l'ordre prévu

J'ai spécifié une rubrique Amazon SNS dans Audit Manager, mais je ne reçois aucune notification

Si votre rubrique Amazon SNS utilise AWS KMS pour le chiffrement côté serveur (SSE), vous ne disposez peut-être pas des autorisations requises pour votre stratégie de clé AWS KMS. Il se peut également que vous ne receviez pas de notifications si vous n'avez pas abonné un point de terminaison à votre rubrique.

Si vous ne recevez pas de notifications, vérifiez que vous avez effectué les opérations suivantes :

- Vous avez joint la politique d'autorisation requise à votre clé KMS. Un exemple de politique est disponible sur la page Notifications de ce guide.

- Vous avez abonné un point de terminaison à la rubrique via laquelle les notifications sont envoyées. Lorsque vous abonnez un point de terminaison de messagerie à une rubrique, vous recevez un e-mail vous demandant de confirmer votre abonnement. Vous devez confirmer votre abonnement pour commencer à recevoir des notifications par e-mail. Pour plus d'informations, consultez Mise en route dans le Guide du développeur d'Amazon SNS.

J'ai spécifié une rubrique FIFO, mais je ne reçois pas de notifications dans l'ordre prévu

Audit Manager prend en charge l'envoi de notifications aux rubriques FIFO SNS. Cependant, l'ordre dans lequel Audit Manager envoie les notifications à vos rubriques FIFO n'est pas garanti.

Résolution des problèmes liés aux autorisations et à l'accès

Vous pouvez utiliser les informations de cette page pour résoudre les problèmes courants d'autorisation dans Audit Manager.

Rubriques

- J'ai suivi la procédure de configuration d'Audit Manager, mais je n'ai pas suffisamment de privilèges IAM
- J'ai désigné une personne comme responsable de l'audit, mais elle n'a toujours pas un accès complet à l'évaluation. Pourquoi est-ce le cas ?
- Je ne parviens pas à exécuter une action dans Audit Manager
- Je veux autoriser des personnes extérieures à mon Compte AWS à accéder à mes ressources Audit Manager
- Voir aussi

J'ai suivi la procédure de configuration d'Audit Manager, mais je n'ai pas suffisamment de privilèges IAM

L'utilisateur, le rôle ou le groupe que vous utilisez pour accéder à Audit Manager doit disposer des autorisations requises. De plus, votre politique basée sur l'identité ne doit pas être trop restrictive. Dans le cas contraire, la console ne fonctionnera pas comme prévu. La procédure de configuration décrite dans ce guide fournit une politique qui accorde les autorisations minimales nécessaires pour configurer Audit Manager. Selon votre cas d'utilisation, vous aurez peut-être besoin d'autorisations

plus larges et moins restrictives. Par exemple, nous recommandons aux responsables de l'audit de disposer d'un accès administrateur. Cela leur permet de modifier les paramètres d'Audit Manager et de gérer des ressources telles que les évaluations, les cadres, les contrôles et les rapports d'évaluation. D'autres utilisateurs, comme les délégués, peuvent n'avoir besoin que d'un accès de gestion ou d'un accès en lecture seule.

Assurez-vous d'ajouter les autorisations appropriées pour votre utilisateur, votre rôle ou votre groupe. Pour les responsables de l'audit, la politique recommandée est AWSAuditManagerAdministratorAccess. Pour les délégués, vous pouvez utiliser l'exemple fourni sur la page des exemples de politiques IAM. Vous pouvez utiliser ces exemples de politiques comme point de départ et apporter les modifications nécessaires pour répondre à vos besoins.

Nous vous recommandons de prendre le temps de personnaliser vos autorisations en fonction de vos besoins spécifiques. Si vous avez besoin d'aide concernant les autorisations IAM, contactez votre administrateur ou AWS Support.

J'ai désigné une personne comme responsable de l'audit, mais elle n'a toujours pas un accès complet à l'évaluation. Pourquoi est-ce le cas ?

Le fait de désigner une personne comme responsable de l'audit ne suffit pas pour lui donner un accès complet à une évaluation. Les responsables de l'audit doivent également disposer des autorisations IAM nécessaires pour accéder aux ressources d'Audit Manager et les gérer. En d'autres termes, en plus de désigner un utilisateur en tant que propriétaire de l'audit, vous devez également associer les politiques IAM nécessaires à cet utilisateur. L'idée sous-jacente est qu'en exigeant les deux, Audit Manager vous garantit un contrôle total sur toutes les spécificités de chaque évaluation.

> **Note**
>
> Pour les responsables de l'audit, nous vous recommandons d'utiliser la politique AWSAuditManagerAdministratorAccess. Pour plus d'informations, consultez Recommended policies for user personas in Audit Manager.

Je ne parviens pas à exécuter une action dans Audit Manager

Si vous ne disposez pas des autorisations nécessaires pour utiliser la console AWS Audit Manager ou les opérations de l'API Audit Manager, il est probable que vous rencontriez une erreur `AccessDeniedException`.

Pour résoudre ce problème, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations de connexion.

Je veux autoriser des personnes extérieures à mon Compte AWS à accéder à mes ressources Audit Manager

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Audit Manager prend en charge ces fonctionnalités, consultez Comment AWS Audit Manager fonctionne avec IAM.
- Pour savoir comment octroyer l'accès à vos ressources à des Comptes AWS dont vous êtes propriétaire, consultez la section Fournir l'accès à un utilisateur IAM dans un autre Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment octroyer l'accès à vos ressources à des Comptes AWS tiers, consultez Fournir l'accès aux Comptes AWS appartenant à des tiers dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des stratégies basées sur les ressources pour l'accès intercompte, veuillez consulter Différence entre les rôles IAM et les stratégies basées sur les ressources dans le Guide de l'utilisateur IAM.

Voir aussi

Les pages suivantes contiennent des conseils pour la résolution d'autres problèmes pouvant être dus à des autorisations manquantes :

- Je ne vois aucun contrôle ou ensemble de contrôles dans mon évaluation
- L'option de règle personnalisée n'est pas disponible lorsque je configure une source de données pour un contrôle

- Je reçois un message d'erreur accès refusé lorsque j'essaie de générer un rapport d'évaluation
- Je reçois un message d'erreur accès refusé lorsque j'essaie de générer un rapport d'évaluation à l'aide de mon compte administrateur délégué
- Je ne parviens pas à activer l'outil de recherche de preuves
- Je ne parviens pas à désactiver l'outil de recherche de preuves
- Ma requête de recherche échoue dans l'outil de recherche de preuves
- J'ai spécifié une rubrique Amazon SNS dans Audit Manager, mais je ne reçois aucune notification

Quotas et restrictions pour AWS Audit Manager

Votre Compte AWS dispose de quotas par défaut, anciennement appelés limites, pour chaque Service AWS. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés.

La plupart des quotas d'Audit Manager sont répertoriés sous l'espace de noms AWS Audit Manager de la console Service Quotas. Pour savoir comment demander une augmentation de quota, consultez Gestion de vos quotas d'Audit Manager.

Quotas par défaut d'Audit Manager

Les quotas AWS Audit Manager suivants sont définis par Compte AWS et par région.

Évaluations

- Nombre d'évaluations actives par compte : 100

Rapports d'évaluation

- Nombre d'éléments de preuve que vous pouvez ajouter à un rapport d'évaluation :
  - Pour les rapports portant sur la même région (où l'évaluation et le compartiment S3 de destination du rapport d'évaluation se trouvent dans le même compartimentRégion AWS) : 22 000
  - Pour les rapports inter-région (où l'évaluation et le compartiment S3 de destination du rapport d'évaluation se trouvent dans le même compartimentRégions AWS) : 3 500
  - Pour les rapports où l'évaluation associée utilise un client géré AWS KMS key : 3 500

Contrôles

- Nombre de tâches simultanées par compte : 500

Eléments probants

- Taille maximale d'un seul fichier de preuve manuel : 100 Mo

- Nombre de téléchargements manuels quotidiens de preuves par contrôle : 100

> **Tip**
>
> Si vous devez télécharger un grand nombre de preuves manuelles vers un seul contrôle, nous vous recommandons de charger vos preuves par lots sur plusieurs jours.

Frameworks

- Nombre de frameworks personnalisés par compte : 100

> **Note**
>
> Les quotas de framework s'appliquent à tous les frameworks personnalisés partagés de votre bibliothèque de frameworks, quelle que soit la personne ayant créé le framework.

Destinataires du framework personnalisé partagé

- Nombre de comptes bénéficiaires actifs : 100

Accès à l'API

- Nombre de transactions par seconde (TPS) sur toutes les API : 20 TPS

Gestion de vos quotas d'Audit Manager

AWS Audit Manager est intégré à Service Quotas, un Service AWS qui vous permet d'afficher et de gérer vos quotas à partir d'un emplacement central. Pour plus d'informations, veuillez consulter Qu'est-ce que Service Quotas? dans le Guide de l'utilisateur Service Quotas. Service Quotas facilite la recherche de la valeur de vos quotas d'Audit Manager.

Pour afficher Service Quotas d'Audit Manager à l'aide de la console

1. Ouvrez la console Service Quotas à l'adresse https://console.aws.amazon.com/servicequotas/.
2. Dans le panneau de navigation, sélectionnez Services AWS.
3. Dans la liste Services AWS, recherchez et sélectionnez AWS Audit Manager.

4. Dans la liste Service Quotas, vous pouvez voir le nom du quota de service, la valeur de quota appliquée (le cas échéant), la valeur de quota AWS par défaut et si le quota est réglable.
5. Pour afficher des informations supplémentaires sur un quota de service, notamment la description, choisissez le nom du quota.
6. (Facultatif) Pour demander une augmentation de quota, sélectionnez le quota que vous souhaitez augmenter, sélectionnez Request quota increase (Demander une augmentation de quota), saisissez ou sélectionnez les informations requises, puis sélectionnez Request (Demander).

Pour de plus amples informations, veuillez consulter Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas.

Sécurité dans AWS Audit Manager

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est 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 AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Audit Manager, voir AWS Services concernés par programme de conformitéAWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par 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 son utilisation AWS Audit Manager. Les rubriques suivantes expliquent comment configurer Audit Manager pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser les ressources de votre Audit Manager.

Rubriques

- Protection des données dans AWS Audit Manager
- Gestion des identités et des accès pour AWS Audit Manager
- Validation de conformité pour AWS Audit Manager
- Résilience dans AWS Audit Manager
- Sécurité de l'infrastructure dans AWS Audit Manager
- AWS Audit Manager et points de terminaison VPC d'interface ()AWS PrivateLink
- Connexion et surveillance AWS Audit Manager
- Analyse de configuration et de vulnérabilité dans AWS Audit Manager

Protection des données dans AWS Audit Manager

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS Audit Manager. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagéeAWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Audit Manager ou un autre outil Services AWS à l'aide de la console, de l'API ou AWS des SDK. AWS CLIToutes les données

que vous saisissez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Outre la recommandation ci-dessus, nous recommandons spécifiquement aux clients d'Audit Manager de ne pas inclure d'informations d'identification sensibles dans les champs au format de texte libre lors de la création d'évaluations, de contrôles personnalisés, de cadres personnalisés et de commentaires de délégation.

Suppression des données d'Audit Manager

Les données d'Audit Manager peuvent être supprimées de plusieurs manières.

Suppression des données lors de la désactivation d'Audit Manager

Lorsque vous désactivez Audit Manager, vous pouvez décider si vous souhaitez supprimer toutes vos données d'Audit Manager. Si vous choisissez de supprimer vos données, elles seront supprimées dans les 7 jours suivant la désactivation d'Audit Manager. Une fois vos données supprimées, vous ne pouvez pas les récupérer.

Suppression automatique des données

Certaines données d'Audit Manager sont supprimées automatiquement après un certain temps. Audit Manager conserve les données des clients comme suit.

Type de données	Période de conservation des données	Remarques
Éléments probants	Les données sont conservées pendant 2 ans à partir de leur création	Cela comprend les éléments probants automatisés et manuels
Ressources créées par le client	Les données sont conservées indéfiniment	Cela comprend les évaluations, les rapports d'évaluation, les contrôles personnalisés et les frameworks personnalisés

Suppression manuelle des données

Vous pouvez supprimer des ressources d'Audit Manager à tout moment. Pour obtenir des instructions, veuillez consulter les sections suivantes :

- Suppression d'une évaluation
  - Voir également : DeleteAssessmentdans la référence deAWS Audit Manager l'API
- Suppression d'un framework personnalisé
  - Voir également : DeleteAssessmentFrameworkdans la référence deAWS Audit Manager l'API
- Suppression d'une demande de partage
  - Voir également : DeleteAssessmentFrameworkSharedans la référence deAWS Audit Manager l'API
- Suppression d'un rapport d'évaluation
  - Voir également : DeleteAssessmentReportdans la référence deAWS Audit Manager l'API
- Suppression d'un contrôle personnalisé
  - Voir également : DeleteControldans la référence deAWS Audit Manager l'API

Pour supprimer d'autres éventuelles données de ressources créées lors de votre utilisation d'Audit Manager, consultez ce qui suit :

- Supprimer un entrepôt de données d'événements dans le Guide de l'utilisateurAWS CloudTrail
- Suppression d'un compartiment dans le Guide de l'utilisateur d'Amazon Simple Storage Service (Amazon S3).

Chiffrement au repos

Pour chiffrer les données au repos, Audit Manager utilise le chiffrement côté serveur Clés gérées par AWS pour tous ses magasins de données et ses journaux.

Vos données sont cryptées sous une clé gérée par le client ou un Clé détenue par AWS, selon les paramètres que vous avez sélectionnés. Si vous ne fournissez pas de clé gérée par le client, Audit Manager utilise un Clé détenue par AWS pour chiffrer votre contenu. Toutes les métadonnées de service dans DynamoDB et Amazon S3 dans Audit Manager sont chiffrées à l'aide d'une Clé détenue par AWS.

Audit Manager chiffre les données comme suit :

- Les métadonnées de service stockées dans Amazon S3 sont chiffrées dans le cadre d'un Clé détenue par AWS SSE-KMS.
- Les métadonnées de service stockées dans DynamoDB sont chiffrées côté serveur à l'aide de KMS et d'une Clé détenue par AWS.
- Votre contenu stocké dans DynamoDB est chiffré côté client à l'aide d'une clé gérée par le client ou d'une Clé détenue par AWS. La clé KMS est basée sur les paramètres que vous avez choisis.
- Votre contenu stocké dans Amazon S3 dans Audit Manager est chiffré à l'aide d'une clé SSE-KMS. La clé KMS dépend des paramètres sélectionnés et peut être une clé gérée par le client ou une Clé détenue par AWS.
- Les rapports d'évaluation publiés dans votre compartiment S3 sont chiffrés comme suit :
  - Si vous avez fourni une clé gérée par le client, vos données sont cryptées à l'aide de SSE-KMS.
  - Si vous avez utilisé le Clé détenue par AWS, vos données sont cryptées à l'aide du SSE-S3.

Chiffrement en transit

Audit Manager fournit des points de terminaison sécurisés et privés pour le chiffrement des données en transit. Les points de terminaison sécurisés et privés permettent AWS de protéger l'intégrité des demandes d'API adressées à Audit Manager.

Transit interservices

Par défaut, toutes les communications interservices sont protégées par un chiffrement utilisant le protocole TLS (Transport Layer Security).

Gestion des clés

Audit Manager prend en charge à la fois Clés détenues par AWS les clés gérées par le client pour chiffrer toutes les ressources d'Audit Manager (évaluations, contrôles, cadres, preuves et rapports d'évaluation enregistrés dans les compartiments S3 de vos comptes).

Nous vous recommandons d'utiliser une clé gérée par le client. Ce faisant, vous pouvez consulter et gérer les clés de chiffrement qui protègent vos données, y compris les journaux concernant leur utilisation dans AWS CloudTrail. Si vous choisissez une clé gérée par le client, Audit Manager crée une attribution sur la clé KMS, afin de pouvoir l'utiliser pour chiffrer votre contenu.

> **Warning**
>
> Après la suppression ou la désactivation d'une clé KMS utilisée pour chiffrer les ressources Audit Manager, vous ne pouvez plus déchiffrer les ressources chiffrées à l'aide de cette clé, ce qui signifie que les données deviennent irrécupérables.
> La suppression d'une clé KMS dans AWS Key Management Service (AWS KMS) est destructrice et potentiellement dangereuse. Pour plus d'informations sur la suppression des clés KMS, consultez la section Suppression AWS KMS keys du guide de l'utilisateurAWS Key Management Service .

Vous pouvez spécifier vos paramètres de chiffrement lorsque vous activez Audit Manager à l' AWS Management Consoleaide de l'API Audit Manager ou du AWS Command Line Interface (AWS CLI). Pour obtenir des instructions, veuillez consulter Activer AWS Audit Manager.

Vous pouvez consulter et modifier vos paramètres de chiffrement à tout moment. Pour obtenir des instructions, veuillez consulter Chiffrement des données.

Pour plus d'informations sur la configuration des clés gérées par le client, consultez la section Création de clés du guide de l'utilisateurAWS Key Management Service .

Gestion des identités et des accès pour AWS Audit Manager

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent les personnes qui peuvent être authentifiées (connectées) et autorisées (dotées d'autorisations) à utiliser des ressources Audit Manager. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion des accès à l'aide de politiques
- Comment AWS Audit Manager fonctionne avec IAM
- Exemples de politiques basées sur l'identité pour AWS Audit Manager

- Prévention du cas de figure de l'adjoint désorienté entre services
- AWS politiques gérées pour AWS Audit Manager
- Résolution des problèmes AWS Audit Manager d'identité et d'accès
- Utilisation de rôles liés à un service pour AWS Audit Manager

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Audit Manager.

Utilisateur du service : si vous utilisez le service Audit Manager pour effectuer votre tâche, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Plus vous utiliserez de fonctionnalités Audit Manager pour effectuer votre travail, plus vous pourriez avoir besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans Audit Manager, veuillez consulter Résolution des problèmes AWS Audit Manager d'identité et d'accès.

Administrateur du service : si vous êtes le responsable des ressources Audit Manager de votre entreprise, vous bénéficiez probablement d'un accès complet à Audit Manager. Il est de votre responsabilité de déterminer les fonctionnalités et ressources Audit Manager auxquelles les utilisateurs de votre service doivent pouvoir accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec Audit Manager, veuillez consulter Comment AWS Audit Manager fonctionne avec IAM.

Administrateur IAM : si vous êtes un administrateur IAM, vous souhaiterez peut-être en savoir plus sur la création de politiques d'accès à Audit Manager. Pour voir des exemples de politiques Audit Manager basées sur l'identité que vous pouvez utiliser dans IAM, veuillez consulter Exemples de politiques basées sur l'identité pour AWS Audit Manager.

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWSdans le guide deConnexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, veuillez consulter Multi-factor authentication (Authentification multifactorielle) dans le Guide de l'utilisateurAWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateurAWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent

des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, veuillez consulter la rubrique Jeux d'autorisations dans le Guide de l'utilisateurAWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWScas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, une fonction de service ou un rôle lié au service.

- Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, l'action que vous effectuez est susceptible de lancer une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
- Fonction du service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWSLe service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité

ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Présentation des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAFPour en savoir plus sur les listes de contrôle d'accès, consultez Présentation des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonction avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations qui en résultent représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus

d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctions d'une organisation, vous pouvez appliquer les politiques de contrôle de service (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWSd'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateurAWS Organizations .
- politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de la séance obtenue 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 remplace l'autorisation. Pour plus d'informations, consultez Politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations obtenues sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment AWS Audit Manager fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Audit Manager, découvrez les fonctionnalités IAM que vous pouvez utiliser avec Audit Manager.

Fonctionnalités IAM que vous pouvez utiliser avec AWS Audit Manager

Fonctionnalité IAM	Prise en charge par Audit Manager
Politiques basées sur l'identité	Oui

Fonctionnalité IAM	Prise en charge par Audit Manager
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d'une politique	Partielle
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Oui
Transmission des sessions d'accès (FAS)	Oui
Fonctions de service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont AWS Audit Manager les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour AWS Audit Manager

Prend en charge les politiques basées sur l'identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, veuillez consulter Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

AWS Audit Manager crée une politique gérée nommée `AWSAuditManagerAdministratorAccess` pour les administrateurs d'Audit Manager. Cette politique accorde un accès administratif complet dans Audit Manager. Les administrateurs peuvent associer cette politique à n'importe quel rôle ou utilisateur existant, ou créer un nouveau rôle avec cette politique.

Politiques recommandées pour les personas utilisateurs dans AWS Audit Manager

AWS Audit Manager vous permet de maintenir la séparation des tâches entre les différents utilisateurs et pour les différents audits en utilisant différentes politiques IAM. Les deux personna dans Audit Manager et leurs politiques recommandées sont définies comme suit.

Persona	Description et politique recommandée
Responsable de l'audit	• Ce personnage doit disposer des autorisations nécessaires pour gérer les évaluations dans AWS Audit Manager. • La stratégie recommandée à utiliser pour ce personnage est la stratégie gérée nommée AWSAuditManagerAdministratorAccess. Vous pouvez utiliser cette politique comme point de départ et définir la portée de ces autorisations en fonction de vos besoins.
Délégué	• Cette persona peut accéder aux séries de contrôles déléguées dans le cadre d'une évaluation. Elle peut mettre à jour l'état du contrôle, ajouter des commentaires, soumettre une série de contrôles pour examen et ajouter des éléments probants au rapport d'évaluation. • La politique recommandée à utiliser pour cette persona est l'exemple de politique suivant : Permettre aux utilisateurs un accès administrateur complet à AWS Audit Manager. Vous pouvez utiliser cette politique comme point de départ et apporter les modifications nécessaires en fonction de vos besoins.

Exemples de politiques basées sur l'identité pour AWS Audit Manager

Pour voir des exemples de politiques basées sur l'identité, consultez Exemples de politiques basées sur l'identité pour AWS Audit Manager.

Politiques basées sur les ressources au sein de AWS Audit Manager

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez Différence entre les rôles IAM et les politiques basées sur une ressource dans le Guide de l'utilisateur IAM.

Actions politiques pour AWS Audit Manager

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des AWS Audit Manager actions, consultez la section Actions définies par AWS Audit Manager dans le Service Authorization Reference.

Les actions de politique en AWS Audit Manager cours utilisent le préfixe suivant avant l'action.

```
auditmanager
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "auditmanager:GetEvidenceDetails",
      "auditmanager:GetEvidenceEventDetails"
         ]
```

Vous pouvez aussi préciser plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Get`, incluez l'action suivante.

```
"Action": "auditmanager:Get*"
```

Pour voir des exemples de politiques basées sur l'identité, consultez Exemples de politiques basées sur l'identité pour AWS Audit Manager.

Ressources politiques pour AWS Audit Manager

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets pour lesquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de AWS Audit Manager ressources et leurs ARN, consultez la section Ressources définies par AWS Audit Manager dans le Service Authorization Reference. Pour connaître les actions permettant de spécifier l'ARN de chaque ressource, consultez la section Actions définies par AWS Audit Manager.

Une évaluation Audit Manager possède le format d'Amazon Resource Name (ARN) suivant :

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/${assessmentId}
```

Une série de contrôles Audit Manager possède le format d'ARN suivant :

```
arn:${Partition}:auditmanager:${Region}:${Account}:assessment/
${assessmentId}controlSet/${controlSetId}
```

Un contrôle Audit Manager possède le format d'ARN suivant :

```
arn:${Partition}:auditmanager:${Region}:${Account}:control/${controlId}
```

Pour de plus amples informations sur les formats d'ARN, veuillez consulter la section Amazon Ressource Names (ARN).

Par exemple, pour spécifier l'évaluation avec l'ID `i-1234567890abcdef0` dans votre instruction, utilisez l'ARN suivant.

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/
i-1234567890abcdef0"
```

Pour spécifier toutes les instances qui appartiennent à un compte spécifique, utilisez le caractère générique (*).

```
"Resource": "arn:aws:auditmanager:us-east-1:123456789012:assessment/*"
```

Certaines actions Audit Manager, comme celles liées à la création de ressources, ne peuvent pas être exécutées sur une ressource précise. Dans ces cas-là, vous devez utiliser le caractère générique (*).

```
"Resource": "*"
```

De nombreuses actions de l'API Audit Manager impliquent plusieurs ressources. Par exemple, `ListAssessments` renvoie une liste de métadonnées d'évaluation accessibles aux personnes actuellement connectées Compte AWS. Par conséquent, un utilisateur doit être autorisé à consulter les évaluations. Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN par des virgules.

```
"Resource": [
      "resource1",
      "resource2"
```

Pour afficher une liste des types de ressources Audit Manager et de leurs ARN, veuillez consulter la section Ressources définies par AWS Audit Manager dans le Guide de l'utilisateur IAM. Pour connaître les actions permettant de spécifier l'ARN de chaque ressource, consultez la section Actions définies par AWS Audit Manager.

Certaines actions de l'API Audit Manager prennent en charge plusieurs ressources. Par exemple, `GetChangeLogs` accède à un `assessmentID`, un `controlID` et un `controlSetId`, donc un principal doit posséder les autorisations nécessaires pour accéder à chacune de ces ressources. Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN par des virgules.

```
"Resource": [
      "assessmentId",
```

```
        "controlId",
        "controlSetId"
```

Clés de conditions de politique pour AWS Audit Manager

Prend en charge les clés de condition de politique spécifiques au service	Partielle

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Lorsque le principal d'une instruction de politique est un principal du serviceAWS, nous vous recommandons vivement d'utiliser les clés de condition globales `aws:SourceArn` ou `aws:SourceAccount` dans la politique. Vous pouvez utiliser ces clés contextuelles de condition globale pour éviter le scénario de l'adjoint désorienté. Les politiques documentées suivantes expliquent l'utilisation des clés contextuelles de condition globale `aws:SourceArn` et `aws:SourceAccount` dans Audit Manager afin d'éviter le problème de l'adjoint désorienté.

- Exemple de politique pour une rubrique SNS utilisée pour les notifications d'Audit Manager
- Exemple de politique de clé KMS utilisée avec une rubrique SNS

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur. Pour plus d'informations, consultez la section Éléments d'une politique IAM : variables et balises dans le Guide de l'utilisateur IAM.

Audit Manager ne fournit pas de clés de condition spécifiques au service, mais prend en charge l'utilisation de certaines clés de condition globales. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de conditionAWS globales dans le guide de l'utilisateur IAM.

Listes de contrôle d'accès (ACL) dans AWS Audit Manager

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Contrôle d'accès basé sur les attributs (ABAC) avec AWS Audit Manager

Prend en charge ABAC (étiquettes dans les politiques)	Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des balises, vous devez fournir les informations de balise dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès basé sur les attributs (ABAC) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur le balisage AWS Audit Manager des ressources, consultezBalisage de ressources AWS Audit Manager.

Utilisation d'informations d'identification temporaires avec AWS Audit Manager

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultezServices AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Transférer les sessions d'accès pour AWS Audit Manager

Prend en charge les transmissions de sessions d'accès (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, l'action que vous effectuez est susceptible de lancer une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Fonctions du service pour AWS Audit Manager

Prend en charge les fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations d'une fonction du service peut altérer la fonctionnalité d' AWS Audit Manager . Ne modifiez des fonctions de service que lorsqu'Amazon ECS vous le conseille.

Rôles liés à un service pour AWS Audit Manager

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWSLe service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus de détails sur les rôles liés à un service pour AWS Audit Manager, consultez. Utilisation de rôles liés à un service pour AWS Audit Manager

Exemples de politiques basées sur l'identité pour AWS Audit Manager

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier des ressources Audit Manager. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par AWS Audit Manager, y compris le format des ARN pour chacun des types de ressources, veuillez consulter Actions, ressources et clés de condition pour AWS Audit Manager dans la Référence de l'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Ajoutez les autorisations minimales requises pour activer Audit Manager
- Permettre aux utilisateurs un accès administrateur complet à AWS Audit Manager
- Autoriser l'accès de gestion des utilisateurs à AWS Audit Manager
- Autoriser les utilisateurs à accéder en lecture seule à AWS Audit Manager
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- AWS Audit Manager Autoriser l'envoi de notifications aux rubriques Amazon SNS
- Autoriser les utilisateurs à exécuter des requêtes de recherche dans l'outil de recherche d'éléments probants

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources Audit Manager dans votre compte. Ces actions peuvent entraîner des frais pour

votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiquesAWS 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 de plus amples informations, consultez Politiques géréesAWS ou Politiques géréesAWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège - Lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez Politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès - Vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour de plus amples informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWSPour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour de plus amples informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Ajoutez les autorisations minimales requises pour activer Audit Manager

Cet exemple montre comment autoriser des comptes sans rôle d'administrateur à activer AWS Audit Manager.

> **Note**
>
> Ce que nous proposons ici est une politique de base accordant les autorisations minimales nécessaires pour activer Audit Manager. Toutes les autorisations définies dans la politique suivante sont requises. Si vous omettez une partie de cette politique, vous ne pourrez pas activer Audit Manager.
> Nous vous recommandons de prendre le temps de personnaliser vos autorisations en fonction de vos besoins spécifiques. Si vous avez encore besoin d'aide, contactez votre administrateur ou AWS Support.

Pour accorder l'accès minimum requis pour activer Audit Manager, utilisez les autorisations suivantes.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "auditmanager:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
```

```
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                   ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Effect": "Allow",
            "Action": "kms:ListAliases",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        }
    ]
}
```

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API que vous tentez d'effectuer.

Permettre aux utilisateurs un accès administrateur complet à AWS Audit Manager

Les exemples de politiques suivants accordent un accès administrateur complet à AWS Audit Manager.

- Exemple 1 (politique gérée, `AWSAuditManagerAdministratorAccess`)
- Exemple 2 (autorisations de destination du rapport d'évaluation)
- Exemple 3 (autorisations de destination d'exportation)
- Exemple 4 (Autorisations pour activer l'outil de recherche d'éléments probants)
- Exemple 5 (Autorisations pour désactiver l'outil de recherche d'éléments probants)

Exemple 1 (politique gérée, **`AWSAuditManagerAdministratorAccess`**)

La politique présentée dans cet exemple est la politique gérée, `AWSAuditManagerAdministratorAccess`. Cette politique inclut la possibilité d'activer et de désactiver Audit Manager, de modifier ses paramètres et de gérer toutes ses ressources comme les évaluations, les frameworks, les contrôles et les rapports d'évaluation.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
```

```
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemple 2 (autorisations de destination du rapport d'évaluation)

Cette politique vous autorise à accéder à un compartiment S3 spécifique, à y ajouter des fichiers et à en supprimer. Cela vous permet d'utiliser le compartiment spécifié comme destination du rapport d'évaluation dans Audit Manager.

Remplacez chaque *espace réservé* par vos propres informations. Incluez le compartiment S3 destination de votre rapport d'évaluation et la clé KMS utilisée pour chiffrer vos rapports d'évaluation.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "s3:PutObject",
               "s3:GetObject",
               "s3:ListBucket",
               "s3:DeleteObject",
               "s3:GetBucketLocation",
               "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
        }
    ]
},
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey"
            ],
```

```
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

Exemple 3 (autorisations de destination d'exportation)

La politique suivante permet de CloudTrail fournir les résultats des requêtes Evidence Finder au compartiment S3 spécifié. En tant que bonne pratique en matière de sécurité, la clé de condition globale IAM `aws:SourceArn` permet de garantir que les CloudTrail écritures dans le compartiment S3 ne sont destinées qu'au magasin de données d'événements.

Remplacez *l'espace réservé* par vos propres informations.

- Remplacez *DOC-EXAMPLE-DESTINATION-BUCKET* par le compartiment S3 utilisé comme destination d'exportation.
- Remplacez *myQueryRunningRegion* par la région appropriée Région AWS à votre configuration.
- Remplacez *MyAccountID* par l' Compte AWS ID utilisé pour. CloudTrail Il se peut qu'il ne soit pas identique à l'ID Compte AWS du compartiment S3. S'il s'agit d'un magasin de données sur les événements d'une organisation, vous devez utiliser le Compte AWS pour le compte de gestion.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
            "Condition": {
                "StringEquals": {
```

```
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemple 4 (Autorisations pour activer l'outil de recherche d'éléments probants)

La politique d'autorisation suivante est requise si vous souhaitez activer et utiliser la fonctionnalité de recherche d'éléments probants. Cette déclaration de politique permet à Audit Manager de créer un magasin de données d'événements CloudTrail Lake et d'exécuter des requêtes de recherche.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
           "Sid": "ManageCloudTrailLakeQueryAccess",
           "Effect": "Allow",
           "Action": [
               "cloudtrail:StartQuery",
               "cloudtrail:DescribeQuery",
               "cloudtrail:GetQueryResults",
               "cloudtrail:CancelQuery"
           ],
           "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
        },
        {
           "Sid": "ManageCloudTrailLakeAccess",
           "Effect": "Allow",
           "Action": [
                "cloudtrail:CreateEventDataStore"
           ],
           "Resource": "arn:aws:cloudtrail:*:*:eventdatastore/*"
         }
    ]
}
```

Exemple 5 (Autorisations pour désactiver l'outil de recherche d'éléments probants)

Cet exemple de politique autorise la désactivation de la fonctionnalité de recherche d'éléments probants dans Audit Manager. Cela implique de supprimer l'entrepôt de données d'événements créé lors de la première activation de cette fonctionnalité.

Pour utiliser cette politique, remplacez le *texte de l'espace réservé* par vos propres informations. Vous devez spécifier l'UUID de l'entrepôt de données d'événements créé lors de l'activation de l'outil de recherche d'éléments probants. Vous pouvez récupérer l'ARN de l'entrepôt de données d'événements à partir de vos paramètres Audit Manager. Pour plus d'informations, consultez GetSettings dans la Référence d'APIAWS Audit Manager .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "cloudtrail:DeleteEventDataStore",
               "cloudtrail:UpdateEventDataStore"
            ],
            "Resource": "arn:aws:cloudtrail:::event-data-store-UUID"
        }
    ]
}
```

Autoriser l'accès de gestion des utilisateurs à AWS Audit Manager

Cet exemple montre comment autoriser un accès de gestion non administrateur à AWS Audit Manager.

Cette politique permet de gérer toutes les ressources d'Audit Manager (évaluations, frameworks et contrôles), mais ne permet pas d'activer ou de désactiver Audit Manager ou de modifier les paramètres d'Audit Manager.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:GetAccountStatus",
                "auditmanager:ListAssessmentFrameworks",
                "auditmanager:CreateAssessmentFramework",
                "auditmanager:GetAssessmentFramework",
                "auditmanager:UpdateAssessmentFramework",
                "auditmanager:DeleteAssessmentFramework",
                "auditmanager:ListAssessmentReports",
                "auditmanager:ListAssessments",
                "auditmanager:CreateAssessment",
                "auditmanager:ListControls",
                "auditmanager:CreateControl",
                "auditmanager:GetControl",
```

```
                "auditmanager:UpdateControl",
                "auditmanager:DeleteControl",
                "auditmanager:ListKeywordsForDataSource",
                "auditmanager:GetDelegations",
                "auditmanager:ValidateAssessmentReportIntegrity",
                "auditmanager:ListNotifications",
                "auditmanager:GetServicesInScope",
                "auditmanager:GetSettings",
                "auditmanager:ListTagsForResource",
                "auditmanager:TagResource",
                "auditmanager:UntagResource"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Autoriser les utilisateurs à accéder en lecture seule à AWS Audit Manager

Cette politique accorde un accès en lecture seule aux AWS Audit Manager ressources telles que les évaluations, les cadres et les contrôles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "auditmanager:Get*",
                "auditmanager:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

AWS Audit Manager Autoriser l'envoi de notifications aux rubriques Amazon SNS

Les politiques de cet exemple accordent à Audit Manager l'autorisation d'envoyer des notifications à une rubrique Amazon SNS existante.

- Exemple 1 : si vous souhaitez recevoir des notifications d'Audit Manager, ajoutez des autorisations à votre stratégie d'accès de rubrique SNS comme dans cet exemple.
- Exemple 2 — Si votre rubrique SNS utilise AWS Key Management Service (AWS KMS) pour le chiffrement côté serveur (SSE), utilisez cet exemple pour ajouter des autorisations à la politique d'accès aux clés KMS.

Dans les politiques suivantes, le principal qui obtient les autorisations est le principal du service Audit Manager, qui est `auditmanager.amazonaws.com`. Lorsque le principal d'une instruction de politique est un principal du serviceAWS, nous vous recommandons vivement d'utiliser les clés de condition globales `aws:SourceArn` ou `aws:SourceAccount` dans la politique. Vous pouvez utiliser ces clés contextuelles de condition globale pour éviter le scénario de l'adjoint désorienté.

Exemple 1 (Autorisations pour la rubrique SNS)

Cette instruction de politique autorise Audit Manager à publier des événements sur la rubrique SNS spécifiée. Toute demande de publication sur la rubrique SNS spécifiée doit satisfaire aux conditions de la politique.

Pour utiliser cette politique, remplacez le *`texte de l'espace réservé`* par vos propres informations. Notez les informations suivantes :

- Si vous utilisez la clé de condition `aws:SourceArn` dans cette politique, la valeur doit être l'ARN de la ressource Audit Manager d'où provient la notification. Dans l'exemple ci-dessous, `aws:SourceArn` utilise un caractère générique (`*`) pour l'ID de ressource. Cela autorise toutes les demandes provenant d'Audit Manager sur toutes les ressources d'Audit Manager. Avec la clé de condition globale `aws:SourceArn`, vous pouvez utiliser l'opérateur de condition `StringLike` ou `ArnLike`. Comme bonne pratique, nous vous recommandons d'utiliser `ArnLike`.

- Avec la clé de condition `aws:SourceAccount`, vous pouvez utiliser l'opérateur de condition `StringEquals` ou `StringLike`. Comme bonne pratique, nous vous recommandons d'utiliser `StringEquals` pour la mise en place du moindre privilège.
- Si vous utilisez à la fois `aws:SourceAccount` et `aws:SourceArn`, les valeurs de compte doivent comporter le même ID de compte.

```
{
  "Version": "2012-10-17",
  "Statement": {
      "Sid": "AllowAuditManagerToUseSNSTopic",
      "Effect": "Allow",
      "Principal": {
        "Service": "auditmanager.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:accountID:topicName",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "accountID"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
    }
}
```

L'exemple alternatif suivant utilise uniquement la clé de condition `aws:SourceArn`, avec l'opérateur de condition `StringLike` :

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:auditmanager:region:accountID:*"
        }
      }
```

L'exemple alternatif suivant utilise uniquement la clé de condition `aws:SourceAccount`, avec l'opérateur de condition `StringLike` :

```
    "Condition": {
```

```
      "StringLike": {
        "aws:SourceAccount": "accountID"
       }
     }
```

Exemple 2 (autorisations pour la clé KMS associée à la rubrique SNS)

L'instruction de politique permet à Audit Manager d'utiliser la clé KMS pour générer la clé de données utilisée pour chiffrer une rubrique SNS. Toute demande d'utilisation de la clé KMS pour l'opération spécifiée doit répondre aux conditions de la politique.

Pour utiliser cette politique, remplacez le *texte de l'espace réservé* par vos propres informations. Notez les informations suivantes :

- Si vous utilisez la clé de condition `aws:SourceArn` dans cette politique, la valeur doit être l'ARN de la ressource chiffrée. Par exemple, dans ce cas, il s'agit de la rubrique SNS de votre compte. Définissez la valeur sur l'ARN ou un modèle d'ARN avec des caractères génériques (*). Avec la clé de condition `aws:SourceArn`, vous pouvez utiliser l'opérateur de condition `StringLike` ou `ArnLike`. Comme bonne pratique, nous vous recommandons d'utiliser `ArnLike`.
- Avec la clé de condition `aws:SourceAccount`, vous pouvez utiliser l'opérateur de condition `StringEquals` ou `StringLike`. Comme bonne pratique, nous vous recommandons d'utiliser `StringEquals` pour la mise en place du moindre privilège. Si vous ne connaissez pas l'ARN de la rubrique SNS, vous pouvez utiliser `aws:SourceAccount`.
- Si vous utilisez à la fois `aws:SourceAccount` et `aws:SourceArn`, les valeurs de compte doivent comporter le même ID de compte.

```
{
     "Version": "2012-10-17",
     "Statement": {
       "Sid": "AllowAuditManagerToUseKMSKey",
       "Effect": "Allow",
       "Principal": {
           "Service": "auditmanager.amazonaws.com"
       },
       "Action": [
           "kms:Decrypt",
           "kms:GenerateDataKey"
       ],
       "Resource": "arn:aws:kms:region:accountID:key/*",
```

```
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "accountID"
             }
             "ArnLike": {
                  "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
             }
       }
     }
   ]
}
```

L'exemple alternatif suivant utilise uniquement la clé de condition `aws:SourceArn`, avec l'opérateur de condition `StringLike` :

```
      "Condition": {
        "StringLike": {
          "aws:SourceArn": "arn:aws:sns:region:accountID:topicName"
        }
      }
```

L'exemple alternatif suivant utilise uniquement la clé de condition `aws:SourceAccount`, avec l'opérateur de condition `StringLike` :

```
   "Condition": {
     "StringLike": {
       "aws:SourceAccount": "accountID"
      }
    }
```

Autoriser les utilisateurs à exécuter des requêtes de recherche dans l'outil de recherche d'éléments probants

La politique suivante accorde des autorisations pour effectuer des requêtes sur un magasin de données d'événements CloudTrail Lake. La politique d'autorisation est requise si vous souhaitez utiliser la fonctionnalité de recherche d'éléments probants.

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "ManageCloudTrailLakeQueryAccess",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartQuery",
                "cloudtrail:DescribeQuery",
                "cloudtrail:GetQueryResults",
                "cloudtrail:CancelQuery"
            ],
            "Resource": "*"
        }
    ]
}
```

Prévention du cas de figure de l'adjoint désorienté entre services

Le problème de l'adjoint confus est un problème de sécurité dans lequel une entité qui n'a pas l'autorisation d'effectuer une action peut contraindre une entité plus privilégiée à effectuer cette action. En AWS, l'usurpation d'identité interservices peut entraîner la confusion des adjoints. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé pour utiliser ses autorisations pour agir sur les ressources d'un autre client, lorsqu'il n'a pas l'autorisation de le faire. Pour éviter cela, Amazon Web Services fournit des outils qui peuvent vous aider à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous recommandons d'utiliser les clés contextuelles de condition `aws:SourceAccount`globale `aws:SourceArn`et les clés contextuelles dans les politiques de ressources afin de limiter les autorisations accordées à un autre service pour accéder à vos ressources. AWS Audit Manager

- Utilisez `aws:SourceArn` si vous souhaitez qu'une seule ressource soit associée à l'accès entre services. Vous pouvez également utiliser `aws:SourceArn` avec un caractère générique (`*`) si vous souhaitez spécifier plusieurs ressources.

  Par exemple, vous pouvez utiliser une rubrique Amazon SNS pour recevoir des notifications d'activité de la part d'Audit Manager. Dans ce cas, dans votre stratégie d'accès à la rubrique SNS, la valeur ARN de `aws:SourceArn` est la ressource Audit Manager d'où provient la notification. Comme il est probable que vous disposiez de plusieurs ressources Audit Manager, nous vous

recommandons d'utiliser `aws:SourceArn` avec un caractère générique. Cela vous permet de spécifier toutes les ressources Audit Manager dans votre stratégie d'accès à la rubrique SNS.

- Utilisez `aws:SourceAccount` si vous souhaitez autoriser l'association d'une ressource de ce compte à l'utilisation interservices.
- Si la valeur `aws:SourceArn` ne contient pas l'ID de compte, tel qu'un ARN de compartiment Amazon S3, vous devez utiliser les deux clés de contexte de condition globale pour limiter les autorisations.
- Si vous utilisez les deux conditions et que la valeur de `aws:SourceArn` contient l'ID de compte, la valeur de `aws:SourceAccount` et le compte indiqué dans la valeur de `aws:SourceArn` doivent utiliser le même ID de compte lorsqu'il est utilisé dans la même déclaration de politique.
- Le moyen le plus efficace de se protéger du problème de l'adjoint désorienté consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource. Si vous ne connaissez pas l'Amazon Resource Name (ARN) complet de la ressource ou spécifiez plusieurs ressources, utilisez la clé de contexte de condition globale `aws:SourceArn` avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Audit Manager : assistance adjoint désorienté

Audit Manager fournit une assistance adjoint désorienté dans les scénarios suivants. L'exemple suivant montre comment utiliser les clés de condition `aws:SourceArn` et `aws:SourceAccount` afin d'éviter le problème de l'adjoint désorienté.

- Exemple de politique : rubrique SNS utilisée pour recevoir les notifications d'Audit Manager
- Exemple de politique : clé KMS utilisée pour chiffrer votre rubrique SNS

Audit Manager ne fournit pas d'assistance adjoint désorienté pour la clé gérée par le client fournie dans vos paramètres Chiffrement des données Audit Manager. Si vous avez fourni votre propre clé gérée par le client, vous ne pouvez pas utiliser les conditions `aws:SourceAccount` ou `aws:SourceArn` énoncées dans cette stratégie de clé KMS.

AWS politiques gérées pour AWS Audit Manager

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation

courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez Politiques gérées parAWS dans le Guide de l'utilisateur IAM.

Rubriques

- AWS politique gérée : AWSAuditManagerAdministratorAccess
- AWS politique gérée : AWSAuditManagerServiceRolePolicy
- AWS Audit Manager mises à jour des politiques AWS gérées

AWS politique gérée : AWSAuditManagerAdministratorAccess

Vous pouvez associer la politique `AWSAuditManagerAdministratorAccess` à vos identités IAM.

Cette politique accorde des autorisations administratives qui permettent un accès administratif complet à AWS Audit Manager. Cet accès inclut la possibilité d'activer et de désactiver AWS Audit Manager, de modifier les paramètres et de gérer toutes les ressources d'Audit Manager, telles que les évaluations, les cadres, les contrôles et les rapports d'évaluation. AWS Audit Manager

AWS Audit Manager nécessite des autorisations étendues sur plusieurs AWS services. Cela est dû au fait qu'il AWS Audit Manager s'intègre à plusieurs AWS services pour collecter automatiquement Compte AWS des preuves à partir des services concernés par une évaluation.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `Audit Manager` – Permet aux principaux d'obtenir des autorisations complètes sur les ressources AWS Audit Manager .
- `Organizations` – Permet aux principaux de répertorier les comptes et les unités organisationnelles, et d'enregistrer ou de désenregistrer un administrateur délégué. Cela est nécessaire pour que vous puissiez activer le support multi-comptes, AWS Audit Manager effectuer des évaluations sur plusieurs comptes et consolider les preuves dans un compte d'administrateur délégué.
- `iam` – Permet aux principaux d'obtenir et de répertorier les utilisateurs dans IAM et de créer un rôle lié à un service. Ceci est nécessaire pour pouvoir désigner les responsables d'audit et les délégués pour une évaluation. Cette politique autorise également les principaux à supprimer le rôle lié à un service et à récupérer l'état de suppression. Cela est nécessaire pour nettoyer les ressources et supprimer le rôle lié au service pour vous lorsque vous choisissez de désactiver le service dans le. AWS Audit Manager AWS Management Console
- `s3` – Permet aux principaux de répertorier les compartiments Amazon Simple Storage Service (Amazon S3) disponibles. Cette fonctionnalité est requise pour désigner le compartiment S3 dans lequel vous souhaitez stocker les rapports d'éléments probants ou télécharger les éléments probants manuels.
- `kms` – Permet aux principaux de répertorier et de décrire les clés, de répertorier les alias et de créer des attributions. Ceci est nécessaire pour choisir des clés gérées par le client pour le chiffrement des données.
- `sns` – Permet aux principaux de répertorier les rubriques d'abonnement dans Amazon SNS. Ceci est nécessaire pour spécifier la rubrique SNS à laquelle vous souhaitez que AWS Audit Manager envoie des notifications.
- `events`— Permet aux principaux de répertorier et de gérer les chèques provenant de AWS Security Hub. Cela est nécessaire pour AWS Audit Manager pouvoir collecter automatiquement AWS Security Hub les résultats des AWS services surveillés par AWS Security Hub. Il peut ensuite convertir ces données en éléments probants à inclure dans vos évaluations AWS Audit Manager .
- `tag` – Permet aux principaux de récupérer les ressources étiquetées. Ceci est nécessaire pour que vous puissiez utiliser les balises comme filtre de recherche lorsque vous parcourez les frameworks, les contrôles et les évaluations dans AWS Audit Manager.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "AuditManagerAccess",
            "Effect": "Allow",
            "Action": [
                "auditmanager:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "OrganizationsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowOnlyAuditManagerIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [
                        "auditmanager.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": [
                "iam:GetUser",
                "iam:ListUsers",
```

```
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMAccessCreateSLR",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "auditmanager.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMAccessManageSLR",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:UpdateRoleDescription",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
auditmanager.amazonaws.com/AWSServiceRoleForAuditManager*"
        },
        {
            "Sid": "S3Access",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KmsAccess",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "KmsCreateGrantAccess",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                },
                "StringLike": {
                    "kms:ViaService": "auditmanager.*.amazonaws.com"
                }
            }
        },
        {
            "Sid": "SNSAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateEventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:PutRule"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:detail-type": "Security Hub Findings - Imported"
                },
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.securityhub"
                    ]
                }
            }
        },
        {
```

```
            "Sid": "EventsAccess",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/
AuditManagerSecurityHubFindingsReceiver"
        },
        {
            "Sid": "TagAccess",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politique gérée : AWSAuditManagerServiceRolePolicy

Vous ne pouvez pas joindre de `AWSAuditManagerServiceRolePolicy` à vos entités IAM. Cette politique est associée à un rôle lié à un service`AWSServiceRoleForAuditManager`, qui permet d' AWS Audit Manager effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter Utilisation des rôles liés à un service pour AWS Audit Manager.

La politique d'autorisation des rôles, `AWSAuditManagerServiceRolePolicy`, permet à AWS Audit Manager de rassembler des éléments probants de manière automatisée en effectuant les opérations suivantes en votre nom :

- Rassembler des données à partir des sources de données suivantes :
  - Événements de gestion de AWS CloudTrail
  - Contrôles de conformité effectués par AWS Config Rules
  - Contrôles de conformité effectués par AWS Security Hub

- Utilisez les appels d'API pour décrire les configurations de vos ressources dans les Services AWSsuivants.

> **Tip**
>
> Pour plus d'informations sur les appels d'API utilisés par Audit Manager pour rassembler des éléments probants provenant de ces services, consultez la section Appels d'API pris en charge pour les sources de données de contrôle personnalisées dans ce guide.

  - AWS Certificate Manager
  - AWS Backup
  - Amazon Bedrock
  - AWS CloudTrail
  - Amazon CloudWatch
  - Amazon CloudWatch Logs
  - Groupes d'utilisateurs Amazon Cognito
  - AWS Config
  - AWS Direct Connect
  - Amazon DynamoDB
  - Amazon EC2
  - Amazon Elastic Container Service
  - Amazon Elastic File System
  - Amazon Elastic Kubernetes Service
  - Amazon ElastiCache
  - Elastic Load Balancing
  - Amazon EMR
  - Amazon EventBridge
  - Amazon Data Firehose
  - Amazon FSx
  - Amazon GuardDuty
  - AWS Identity and Access Management (JE SUIS)

- Amazon Kinesis
- AWS KMS
- AWS Lambda
- AWS License Manager
- Amazon Managed Streaming for Apache Kafka
- AWS Organizations
- Amazon Relational Database Service
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- AWS Security Hub
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- AWS WAF

Détails de l'autorisation

`AWSAuditManagerServiceRolePolicy`permet AWS Audit Manager de réaliser les actions suivantes sur les ressources spécifiées :

- `acm:GetAccountConfiguration`
- `acm:ListCertificates`
- `backup:ListRecoveryPointsByResource`
- `bedrock:GetCustomModel`
- `bedrock:GetFoundationModel`
- `bedrock:GetModelCustomizationJob`
- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:ListCustomModels`
- `bedrock:ListFoundationModels`
- `bedrock:ListModelCustomizationJobs`
- `cloudtrail:DescribeTrails`
- `cloudtrail:LookupEvents`

- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- config:DescribeConfigRules
- config:DescribeDeliveryChannels
- config:ListDiscoveredResources
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeTable
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways

- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets

- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors
- iam:GenerateCredentialReport
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions

- `license-manager:ListAssociationsForLicenseConfiguration`
- `license-manager:ListLicenseConfigurations`
- `license-manager:ListUsageForLicenseConfiguration`
- `logs:DescribeDestinations`
- `logs:DescribeExportTasks`
- `logs:DescribeLogGroups`
- `logs:DescribeMetricFilters`
- `logs:DescribeResourcePolicies`
- `logs:FilterLogEvents`
- `organizations:DescribeOrganization`
- `organizations:DescribePolicy`
- `rds:DescribeCertificates`
- `rds:DescribeDbClusterEndpoints`
- `rds:DescribeDbClusterParameterGroups`
- `rds:DescribeDbClusters`
- `rds:DescribeDBInstances`
- `rds:DescribeDbSecurityGroups`
- `redshift:DescribeClusters`
- `route53:GetQueryLoggingConfig`
- `s3:GetBucketPolicy`
  - Cette action d'API fonctionne dans le cadre de l' Compte AWS endroit où elle service-linked-role est disponible. Elle ne peut pas accéder aux politiques de compartiments intercompte.
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketVersioning`
- `s3:GetEncryptionConfiguration`
- `s3:GetLifecycleConfiguration`
- `s3:ListAllMyBuckets`
- `securityhub:DescribeStandards`
- `sns:ListTopics`
- `sqs:ListQueues`

- waf-regional:GetLoggingConfiguration
- waf-regional:ListRuleGroups
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:ListActivatedRulesInRuleGroup

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "acm:GetAccountConfiguration",
    "acm:ListCertificates",
    "backup:ListRecoveryPointsByResource",
    "bedrock:GetCustomModel",
    "bedrock:GetFoundationModel",
    "bedrock:GetModelCustomizationJob",
    "bedrock:GetModelInvocationLoggingConfiguration",
    "bedrock:ListCustomModels",
    "bedrock:ListFoundationModels",
    "bedrock:ListModelCustomizationJobs",
    "cloudtrail:DescribeTrails",
    "cloudtrail:LookupEvents",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:DescribeAlarmsForMetric",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cognito-idp:DescribeUserPool",
    "config:DescribeConfigRules",
    "config:DescribeDeliveryChannels",
    "config:ListDiscoveredResources",
    "directconnect:DescribeDirectConnectGateways",
    "directconnect:DescribeVirtualGateways",
    "dynamodb:DescribeTable",
    "dynamodb:ListBackups",
    "dynamodb:ListGlobalTables",
    "dynamodb:ListTables",
    "ec2:DescribeAddresses",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeEgressOnlyInternetGateways",
```

```
    "ec2:DescribeFlowLogs",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations",
    "ec2:DescribeLocalGateways",
    "ec2:DescribeLocalGatewayVirtualInterfaces",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetEbsDefaultKmsKeyId",
    "ec2:GetEbsEncryptionByDefault",
    "ecs:DescribeClusters",
    "eks:DescribeAddonVersions",
    "elasticache:DescribeCacheClusters",
    "elasticache:DescribeServiceUpdates",
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeFileSystems",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeSslPolicies",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticmapreduce:ListClusters",
    "elasticmapreduce:ListSecurityConfigurations",
    "events:DescribeRule",
    "events:ListConnections",
    "events:ListEventBuses",
    "events:ListEventSources",
    "events:ListRules",
    "firehose:ListDeliveryStreams",
    "fsx:DescribeFileSystems",
    "guardduty:ListDetectors",
    "iam:GenerateCredentialReport",
    "iam:GetAccountAuthorizationDetails",
    "iam:GetAccountPasswordPolicy",
    "iam:GetAccountSummary",
    "iam:GetCredentialReport",
```

```
    "iam:ListEntitiesForPolicy",
    "iam:ListGroupPolicies",
    "iam:ListGroups",
    "iam:ListOpenIdConnectProviders",
    "iam:ListPolicies",
    "iam:ListRolePolicies",
    "iam:ListRoles",
    "iam:ListSamlProviders",
    "iam:ListUserPolicies",
    "iam:ListUsers",
    "iam:ListVirtualMFADevices",
    "kafka:ListClusters",
    "kafka:ListKafkaVersions",
    "kinesis:ListStreams",
    "kms:DescribeKey",
    "kms:GetKeyPolicy",
    "kms:GetKeyRotationStatus",
    "kms:ListGrants",
    "kms:ListKeyPolicies",
    "kms:ListKeys",
    "lambda:ListFunctions",
    "license-manager:ListAssociationsForLicenseConfiguration",
    "license-manager:ListLicenseConfigurations",
    "license-manager:ListUsageForLicenseConfiguration",
    "logs:DescribeDestinations",
    "logs:DescribeExportTasks",
    "logs:DescribeLogGroups",
    "logs:DescribeMetricFilters",
    "logs:DescribeResourcePolicies",
    "logs:FilterLogEvents",
    "organizations:DescribeOrganization",
    "organizations:DescribePolicy",
    "rds:DescribeCertificates",
    "rds:DescribeDbClusterEndpoints",
    "rds:DescribeDbClusterParameterGroups",
    "rds:DescribeDbClusters",
    "rds:DescribeDBInstances",
    "rds:DescribeDbSecurityGroups",
    "redshift:DescribeClusters",
    "route53:GetQueryLoggingConfig",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketVersioning",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
```

```
    "s3:ListAllMyBuckets",
    "securityhub:DescribeStandards",
    "sns:ListTopics",
    "sqs:ListQueues",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:ListRuleGroups",
    "waf-regional:ListSubscribedRuleGroups",
    "waf-regional:ListWebACLs",
    "waf:ListActivatedRulesInRuleGroup"
   ],
   "Resource": "*",
   "Sid": "AuditManagerAPICallAccess"
  },
  {
   "Sid": "AuditManagerS3GetBucketPolicyAccess",
   "Effect": "Allow",
   "Action": [
    "s3:GetBucketPolicy"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": [
      "${aws:PrincipalAccount}"
     ]
    }
   }
  },
  {
   "Sid": "CreateEventsAccess",
   "Effect": "Allow",
   "Action": [
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver",
   "Condition": {
    "StringEquals": {
     "events:detail-type": "Security Hub Findings - Imported"
    },
    "Null": {
     "events:source": "false"
    },
    "ForAllValues:StringEquals": {
     "events:source": [
```

```
      "aws.securityhub"
     ]
    }
   }
  },
  {
   "Sid": "EventsAccess",
   "Effect": "Allow",
   "Action": [
    "events:DeleteRule",
    "events:DescribeRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:ListTargetsByRule",
    "events:PutTargets",
    "events:RemoveTargets"
   ],
   "Resource": "arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver"
  }
 ]
}
```

AWS Audit Manager mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AWS Audit Manager depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Historique du AWS Audit Manager document.

Modification	Description	Date
AWSAuditManagerServiceRolePolicy – Mise à jour d'une politique existante	Le rôle lié au service permet désormais d' AWS Audit Manager effectuer l'`s3:GetBucketPolicy` action. Cette action d'API est nécessaire pour prendre en charge le framework des bonnes pratiques en matière d'IA générativeAWS v1. Cela permet à Audit Manager de collecter des preuves automatisées concernant les restricti	12/06/2023

Modification	Description	Date
	ons de politiques relatives aux jeux de données d’entraînement de vos modèles d’IA générative. L'`GetBucketPolicy` action fonctionne dans le cadre de l' Compte AWS endroit où elle service-linked-role est disponible. Elle ne peut pas accéder aux politiques de compartiments intercompte.	

Modification	Description	Date
AWSAuditManagerServiceRolePolicy – Mise à jour d'une politique existante	Nous avons ajouté les autorisations suivantes àAWSAuditManagerServiceRolePolicy . AWS Audit Manager peut désormais effectuer les actions suivantes pour collecter des preuves automatisées sur les ressources de votre Compte AWS. • acm:GetAccountConfiguration • acm:ListCertificates • backup:ListRecoveryPointsByResource • bedrock:GetCustomModel • bedrock:GetFoundationModel • bedrock:GetModelCustomizationJob • bedrock:GetModelInvocationLoggingConfiguration • bedrock:ListCustomModels • bedrock:ListFoundationModels • bedrock:ListModelCustomizationJobs • cloudtrail:LookupEvents • cloudwatch:DescribeAlarmsForMetric • cloudwatch:GetMetricStatistics • cloudwatch:ListMetrics • directconnect:DescribeDirectConnectGateways • directconnect:DescribeVirtualGateways • dynamodb:ListBackups	06/11/2023

Modification	Description	Date
	• dynamodb:ListGlobalTables • ec2:DescribeAddresses • ec2:DescribeCustomerGateways • ec2:DescribeEgressOnlyInternetGateways • ec2:DescribeInternetGateways • ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations • ec2:DescribeLocalGateways • ec2:DescribeLocalGatewayVirtualInterfaces • ec2:DescribeNatGateways • ec2:DescribeTransitGateways • ec2:DescribeVpcPeeringConnections • ec2:DescribeVpnConnections • ec2:DescribeVpnGateways • ec2:GetEbsDefaultKmsKeyId • ec2:GetEbsEncryptionByDefault • ecs:DescribeClusters • eks:DescribeAddonVersions • elasticache:DescribeCacheClusters • elasticache:DescribeServiceUpdates • elasticfilesystem:DescribeAccessPoints • elasticloadbalancing:DescribeLoadBalancers	

Modification	Description	Date
	• elasticloadbalancing:DescribeSslPolicies • elasticloadbalancing:DescribeTargetGroups • elasticmapreduce:ListClusters • elasticmapreduce:ListSecurityConfigurations • events:ListConnections • events:ListEventBuses • events:ListEventSources • events:ListRules • firehose:ListDeliveryStreams • fsx:DescribeFileSystems • iam:GetAccountPasswordPolicy • iam:GetCredentialReport • iam:ListOpenIdConnectProviders • iam:ListSamlProviders • iam:ListVirtualMFADevices • kafka:ListClusters • kafka:ListKafkaVersions • kinesis:ListStreams • lambda:ListFunctions • logs:DescribeDestinations • logs:DescribeExportTasks • logs:DescribeLogGroups • logs:DescribeMetricFilters • logs:DescribeResourcePolicies • logs:FilterLogEvents • rds:DescribeCertificates	

Modification	Description	Date
	• rds:DescribeDbClusterEndpoints • rds:DescribeDbClusterParameterGroups • rds:DescribeDbClusters • rds:DescribeDbSecurityGroups • redshift:DescribeClusters • s3:GetBucketPublicAccessBlock • s3:GetBucketVersioning • sns:ListTopics • sqs:ListQueues • waf-regional:GetLoggingConfiguration • waf-regional:ListRuleGroups • waf-regional:ListSubscribedRuleGroups • waf-regional:ListWebACLs	
AWSAuditManagerServiceRolePolicy – Mise à jour d'une politique existante	Nous avons ajouté à AWSAuditManagerServiceRolePolicy les autorisations suivantes : • dynamodb:DescribeTable • dynamodb:ListTables • ec2:DescribeVolumes • kms:GetKeyPolicy • kms:GetKeyRotationStatus • kms:ListKeyPolicies • rds:DescribeDBInstances • redshift:DescribeClusters • s3:GetEncryptionConfiguration • s3:ListAllMyBuckets	07/07/2022

Modification	Description	Date
AWSAuditManagerServiceRolePolicy - mise à jour d'une politique existante	Le rôle lié au service permet désormais d' AWS Audit Manager effectuer l'`organizations:DescribeOrganization` action. Nous avons également réduit la ressource `CreateEventsAccess` d'un caractère générique (`*`) à un type de ressource spécifique (`arn:aws:events:*:*:rule/AuditManagerSecurityHubFindingsReceiver`). Enfin, nous avons ajouté un opérateur de condition `Null` pour la clé de condition `events:source` afin de vérifier qu'une valeur source existe et que sa valeur n'est pas nulle.	20/05/2022
AWSAuditManagerAdministratorAccess - mise à jour d'une politique existante	Nous avons mis à jour la politique relative aux conditions de clés pour `events:source` pour indiquer qu'il s'agit d'une clé à valeurs multiples .	29/04/2022
AWSAuditManagerServiceRolePolicy - mise à jour d'une politique existante	Nous avons mis à jour la politique relative aux conditions de clés pour `events:source` pour indiquer qu'il s'agit d'une clé à valeurs multiples .	16/03/2022
AWS Audit Manager a commencé à suivre les modifications	AWS Audit Manager a commencé à suivre les modifications apportées AWS à ses politiques gérées.	06/05/2021

Résolution des problèmes AWS Audit Manager d'identité et d'accès

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Audit Manager et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AWS Audit Manager
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AWS Audit Manager ressources

Je ne suis pas autorisé à effectuer une action dans AWS Audit Manager

L'`AccessDeniedException`erreur apparaît lorsqu'un utilisateur n'est pas autorisé à utiliser AWS Audit Manager les opérations de l'API Audit Manager.

Dans ce cas, votre administrateur doit mettre à jour la politique pour autoriser votre accès.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter l'action `iam:PassRole`, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à Audit Manager.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Audit Manager. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les stratégies de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AWS Audit Manager ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Audit Manager prend en charge ces fonctionnalités, consultez Comment AWS Audit Manager fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Utilisation de rôles liés à un service pour AWS Audit Manager

AWS Audit Manager utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM lié directement à Audit Manager. Les rôles liés à un service sont prédéfinis par Audit Manager et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration AWS Audit Manager car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Audit Manager définit les autorisations de ses rôles liés à un service ; sauf définition contraire, seul Audit Manager peut endosser ses rôles. Les autorisations

définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez AWS Services qui fonctionnent avec IAM et recherchez les services avec un Oui dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour AWS Audit Manager

Audit Manager utilise le rôle lié au service nommé**`AWSServiceRoleForAuditManager`**, qui permet d'accéder aux services AWS et aux ressources utilisés ou gérés par. AWS Audit Manager

Le rôle lié à un service `AWSServiceRoleForAuditManager` fait confiance au service `auditmanager.amazonaws.com` pour endosser le rôle.

La politique d'autorisation des rôles permet à Audit Manager de collecter des preuves automatisées concernant votre AWS utilisation. `AWSAuditManagerServiceRolePolicy` Plus précisément, il peut effectuer les actions suivantes en votre nom.

- L'Audit Manager peut l'utiliser AWS Security Hub pour collecter des preuves de contrôle de conformité. Dans ce cas, Audit Manager utilise l'autorisation suivante pour signaler les résultats des contrôles de sécurité directement depuis AWS Security Hub. Il joint ensuite les résultats à vos contrôles d'évaluation pertinents à titre d'éléments probants.
  - `securityhub:DescribeStandards`

  > **Note**
  >
  > Pour plus d'informations sur les contrôles Security Hub spécifiques qu'Audit Manager peut décrire, consultez la section AWS Security Hub Contrôles pris en charge par AWS Audit Manager.

- L'Audit Manager peut l'utiliser AWS Config pour collecter des preuves de contrôle de conformité. Dans ce cas, Audit Manager utilise les autorisations suivantes pour communiquer les résultats des évaluations des AWS Config règles directement à partir de AWS Config. Il joint ensuite les résultats à vos contrôles d'évaluation pertinents à titre d'éléments probants.
  - `config:DescribeConfigRules`
  - `config:DescribeDeliveryChannels`

- `config:ListDiscoveredResources`

> **Note**
>
> Pour plus d'informations sur les AWS Config règles spécifiques qu'Audit Manager peut décrire, consultez la section AWS Config Règles prises en charge par AWS Audit Manager.

- Audit Manager peut être utilisé AWS CloudTrail pour collecter des preuves de l'activité des utilisateurs. Dans ce cas, Audit Manager utilise les autorisations suivantes pour capturer l'activité des utilisateurs à partir CloudTrail des journaux. Il joint ensuite l'activité à vos contrôles d'évaluation pertinents à titre d'élément probant.
  - `cloudtrail:DescribeTrails`
  - `cloudtrail:LookupEvents`

> **Note**
>
> Pour plus d'informations sur les CloudTrail événements spécifiques qu'Audit Manager peut décrire, consultez les nomsAWS CloudTrail d'événements pris en charge par AWS Audit Manager.

- Audit Manager peut utiliser des appels AWS d'API pour collecter des preuves de configuration des ressources. Dans ce cas, Audit Manager utilise les autorisations suivantes pour appeler des API en lecture seule décrivant vos configurations de ressources pour les Services AWSsuivants. Il joint ensuite les réponses de l'API à vos contrôles d'évaluation pertinents à titre d'éléments probants.
  - `acm:GetAccountConfiguration`
  - `acm:ListCertificates`
  - `backup:ListRecoveryPointsByResource`
  - `bedrock:GetCustomModel`
  - `bedrock:GetFoundationModel`
  - `bedrock:GetModelCustomizationJob`
  - `bedrock:GetModelInvocationLoggingConfiguration`
  - `bedrock:ListCustomModels`
  - `bedrock:ListFoundationModels`
  - `bedrock:ListModelCustomizationJobs`

- cloudwatch:DescribeAlarms
- cloudwatch:DescribeAlarmsForMetric
- cloudwatch:GetMetricStatistics
- cloudwatch:ListMetrics
- cognito-idp:DescribeUserPool
- directconnect:DescribeDirectConnectGateways
- directconnect:DescribeVirtualGateways
- dynamodb:DescribeTable
- dynamodb:ListBackups
- dynamodb:ListGlobalTables
- dynamodb:ListTables
- ec2:DescribeAddresses
- ec2:DescribeCustomerGateways
- ec2:DescribeEgressOnlyInternetGateways
- ec2:DescribeFlowLogs
- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations
- ec2:DescribeLocalGateways
- ec2:DescribeLocalGatewayVirtualInterfaces
- ec2:DescribeNatGateways
- ec2:DescribeNetworkAcls
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTransitGateways
- ec2:DescribeVolumes
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs

- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:GetEbsDefaultKmsKeyId
- ec2:GetEbsEncryptionByDefault
- ecs:DescribeClusters
- eks:DescribeAddonVersions
- elasticache:DescribeCacheClusters
- elasticache:DescribeServiceUpdates
- elasticfilesystem:DescribeAccessPoints
- elasticfilesystem:DescribeFileSystems
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeSslPolicies
- elasticloadbalancing:DescribeTargetGroups
- elasticmapreduce:ListClusters
- elasticmapreduce:ListSecurityConfigurations
- events:DeleteRule
- events:DescribeRule
- events:DisableRule
- events:EnableRule
- events:ListConnections
- events:ListEventBuses
- events:ListEventSources
- events:ListRules
- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:RemoveTargets
- firehose:ListDeliveryStreams
- fsx:DescribeFileSystems
- guardduty:ListDetectors

- iam:GenerateCredentialReport
- iam:GetAccountAuthorizationDetails
- iam:GetAccountPasswordPolicy
- iam:GetAccountSummary
- iam:GetCredentialReport
- iam:ListEntitiesForPolicy
- iam:ListGroupPolicies
- iam:ListGroups
- iam:ListOpenIdConnectProviders
- iam:ListPolicies
- iam:ListRolePolicies
- iam:ListRoles
- iam:ListSamlProviders
- iam:ListUserPolicies
- iam:ListUsers
- iam:ListVirtualMFADevices
- kafka:ListClusters
- kafka:ListKafkaVersions
- kinesis:ListStreams
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:GetKeyRotationStatus
- kms:ListGrants
- kms:ListKeyPolicies
- kms:ListKeys
- lambda:ListFunctions
- license-manager:ListAssociationsForLicenseConfiguration
- license-manager:ListLicenseConfigurations
- license-manager:ListUsageForLicenseConfiguration
- logs:DescribeDestinations

- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeMetricFilters
- logs:DescribeResourcePolicies
- logs:FilterLogEvents
- organizations:DescribeOrganization
- organizations:DescribePolicy
- rds:DescribeCertificates
- rds:DescribeDbClusterEndpoints
- rds:DescribeDbClusterParameterGroups
- rds:DescribeDbClusters
- rds:DescribeDBInstances
- rds:DescribeDbSecurityGroups
- redshift:DescribeClusters
- route53:GetQueryLoggingConfig
- s3:GetBucketPolicy
  - Cette action d'API fonctionne dans le cadre de l' Compte AWS endroit où elle service-linked-role est disponible. Elle ne peut pas accéder aux politiques de compartiments intercompte.
- s3:GetBucketPublicAccessBlock
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetLifecycleConfiguration
- s3:ListAllMyBuckets
- sns:ListTopics
- sqs:ListQueues
- waf-regional:GetLoggingConfiguration
- waf-regional:ListRuleGroups
- waf-regional:ListSubscribedRuleGroups
- waf-regional:ListWebACLs
- waf:ListActivatedRulesInRuleGroup

> **Note**
>
> Pour plus d'informations sur les appels d'API spécifiques qu'Audit Manager peut décrire, veuillez consulter Appels d'API pris en charge pour les sources de données de contrôle personnalisées.

Pour consulter les détails complets des autorisations du rôle lié au service`AWSServiceRoleForAuditManager`, consultez le Guide de référence des politiques`AWSAuditManagerServiceRolePolicy`AWS gérées.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création du rôle lié à AWS Audit Manager un service

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous l'activez AWS Audit Manager, le service crée automatiquement le rôle lié au service pour vous. Vous pouvez activer Audit Manager depuis la page d'accueil du AWS Management Console, ou via l'API ou AWS CLI. Pour plus d'informations, consultez la section Activer AWS Audit Manager de ce guide.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte.

Modification du rôle lié à AWS Audit Manager un service

AWS Audit Manager ne vous permet pas de modifier le rôle `AWSServiceRoleForAuditManager` lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour en savoir plus, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Pour permettre à une entité IAM de modifier la description du rôle lié à un service **`AWSServiceRoleForAuditManager`**

Ajoutez l'instruction suivante à la stratégie d'autorisation de l'entité IAM qui doit modifier la description d'un rôle lié à un service.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/auditmanager.amazonaws.com/
AWSServiceRoleForAuditManager*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "auditmanager.amazonaws.com"}}
}
```

Supprimer le rôle lié à AWS Audit Manager un service

Si vous n'utilisez plus Audit Manager, nous vous recommandons de supprimer le rôle lié à un service `AWSServiceRoleForAuditManager`. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer votre rôle lié à un service avant de pouvoir le supprimer.

Nettoyage du rôle lié au service

Avant de pouvoir utiliser IAM pour supprimer un rôle lié à un service Audit Manager, vous devez d'abord vérifier qu'aucune session n'est active pour le rôle et supprimer toutes les ressources utilisées par le rôle. Pour ce faire, assurez-vous que l'Audit Manager est complètement désenregistré. Régions AWSAprès le désenregistrement, Audit Manager n'utilise plus le rôle lié au service.

Pour obtenir des instructions sur le désenregistrement d'Audit Manager, veuillez consulter les ressources suivantes :

- Désactiver AWS Audit Manager dans ce guide
- DeregisterAccount dans la Référence d'APIAWS Audit Manager
- désenregistrer un compte dans la référence pourAWS CLI AWS Audit Manager

Pour savoir comment supprimer manuellement les ressources d'Audit Manager, consultez la section Suppression des données d'Audit Manager dans ce guide.

Suppression du rôle lié à un service

Vous pouvez supprimer le rôle lié à un service à l'aide de la console IAM, de l' AWS Command Line Interface (AWS CLI) ou de l'API IAM.

IAM console

Suivez les étapes suivantes pour supprimer le rôle lié à un service dans la console IAM.

Pour supprimer un rôle lié à un service (console)

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation de la console IAM, sélectionnez Roles (Rôles). Sélectionnez la case à cocher en regard de `AWSServiceRoleForAuditManager`, et non le nom ou la ligne.
3. Sous Actions de rôle en haut de la page, sélectionnez Supprimer.
4. Dans la boîte de dialogue de confirmation, vérifiez les dernières informations consultées, indiquant le moment où chacun des rôles sélectionnés a accédé en dernier à un Service AWS. Cela vous permet de confirmer si le rôle est actif actuellement. Si vous souhaitez continuer, saisissez **`AWSServiceRoleForAuditManager`** dans le champ à renseigner, et choisissez Supprimer pour lancer la suppression du rôle lié au service.
5. Consultez les notifications de la console IAM pour surveiller la progression de la suppression du rôle lié à un service. Dans la mesure où la suppression du rôle lié à un service IAM est asynchrone, une fois que vous soumettez le rôle afin qu'il soit supprimé, la suppression peut réussir ou échouer. Si la tâche réussit, le rôle est supprimé de la liste et une notification de succès s'affiche en haut de la page.

AWS CLI

Vous pouvez utiliser les commandes IAM depuis le AWS CLI pour supprimer un rôle lié à un service.

Pour supprimer un rôle lié à un service (AWS CLI)

1. Saisissez la commande suivante pour répertorier le rôle dans votre compte :

```
aws iam get-role --role-name AWSServiceRoleForAuditManager
```

2. Un rôle lié à un service ne pouvant pas être supprimé s'il est utilisé ou si des ressources lui sont associées, vous devez envoyer une demande de suppression. Cette demande peut être refusée si ces conditions ne sont pas remplies. Vous devez capturer le `deletion-task-id` de la réponse afin de vérifier l'état de la tâche de suppression.

Saisissez la commande suivante pour envoyer une demande de suppression d'un rôle lié à un service :

```
aws iam delete-service-linked-role --role-name AWSServiceRoleForAuditManager
```

3. Saisissez la commande suivante pour vérifier l'état de la tâche de suppression :

```
aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
```

L'état de la tâche de suppression peut être `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED` ou `FAILED`. Si la suppression échoue, l'appel renvoie le motif de l'échec, afin que vous puissiez apporter une solution.

IAM API

Vous pouvez utiliser l'API IAM pour supprimer un rôle lié à un service.

Pour supprimer un rôle lié à un service (API)

1. Appelez GetRolepour répertorier le rôle dans votre compte. Dans la demande, spécifiez `AWSServiceRoleForAuditManager` en tant que `RoleName`.
2. Un rôle lié à un service ne pouvant pas être supprimé s'il est utilisé ou si des ressources lui sont associées, vous devez envoyer une demande de suppression. Cette demande peut être refusée si ces conditions ne sont pas remplies. Vous devez capturer le `DeletionTaskId` de la réponse afin de vérifier l'état de la tâche de suppression.

   Pour envoyer une demande de suppression pour un rôle lié à un service, appelez DeleteServiceLinkedRole. Dans la demande, spécifiez `AWSServiceRoleForAuditManager` en tant que `RoleName`.
3. Pour vérifier l'état de la suppression, appelez GetServiceLinkedRoleDeletionStatus. Dans la demande, spécifiez le `DeletionTaskId`.

   L'état de la tâche de suppression peut être `NOT_STARTED`, `IN_PROGRESS`, `SUCCEEDED` ou `FAILED`. Si la suppression échoue, l'appel renvoie le motif de l'échec, afin que vous puissiez apporter une solution.

> **Tip**
>
> La suppression échoue si le service Audit Manager utilise le rôle ou dispose de ressources associées. Cela ne se produit que si vous êtes toujours inscrit auprès d'Audit Manager dans une ou plusieurs Régions AWS. Après le désenregistrement, Audit Manager n'utilise plus le rôle lié au service.
> Pour résoudre un problème de suppression ayant échoué, assurez-vous d'abord d'avoir désenregistré Audit Manager sur tous les sites Régions AWS où vous avez utilisé le service. Ensuite, suivez à nouveau les étapes de la procédure précédente.

Régions prises en charge pour les rôles AWS Audit Manager liés à un service

AWS Audit Manager prend en charge l'utilisation de rôles liés au service partout Régions AWS où le service est disponible. Pour plus d'informations, consultez Points de terminaison du serviceAWS.

Validation de conformité pour AWS Audit Manager

Pour savoir si un programmeServices AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultezServices AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité ProgrammesAWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide duAWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans AWS Audit Manager

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 InfrastructureAWS mondiale.

Sécurité de l'infrastructure dans AWS Audit Manager

En tant que service géré, AWS Audit Manager est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité duAWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à AWS Audit Manager via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Vous pouvez appeler ces opérations d'API depuis n'importe quel emplacement réseau, mais AWS Audit Manager elles prennent en charge les politiques d'accès basées sur les ressources, qui peuvent inclure des restrictions basées sur l'adresse IP source. Vous pouvez également utiliser des politiques Audit Manager pour contrôler l'accès à partir de points de terminaison Amazon Virtual Private Cloud (Amazon VPC) ou de VPC spécifiques. En fait, cela isole l'accès réseau à une ressource Audit Manager donnée uniquement du VPC spécifique au sein AWS du réseau.

AWS Audit Manager et points de terminaison VPC d'interface ()AWS PrivateLink

Vous pouvez établir une connexion privée entre votre VPC et créer un point de AWS Audit Manager terminaison VPC d'interface. Les points de terminaison d'interface sont alimentés par AWS

PrivateLink, une technologie qui vous permet d'accéder en privé aux API Audit Manager sans passerelle Internet, périphérique NAT, connexion VPN ou connexion AWS Direct Connect. Les instances de votre VPC ne requièrent pas d'adresses IP publiques pour communiquer avec les API Audit Manager. Le trafic entre votre VPC et celui qui AWS Audit Manager ne quitte pas le AWS réseau.

Chaque point de terminaison d'interface est représenté par une ou plusieurs interfaces réseau Elastic dans vos sous-réseaux.

Pour de plus amples informations, consultez Points de terminaison VPC (AWS PrivateLink) dans le Guide de l'utilisateur Amazon VPC.

Considérations relatives aux points de AWS Audit Manager terminaison VPC

Avant de configurer un point de terminaison VPC d'interface pour AWS Audit Manager, assurez-vous de consulter les propriétés et les limites du point de terminaison d'interface dans le guide de l'utilisateur Amazon VPC.

AWS Audit Manager permet d'appeler toutes ses actions d'API depuis votre VPC.

Création d'un point de terminaison de VPC d'interface pour AWS Audit Manager

Vous pouvez créer un point de terminaison VPC pour le AWS Audit Manager service à l'aide de la console Amazon VPC ou du (). AWS Command Line Interface AWS CLIPour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Créez un point de terminaison VPC à l' AWS Audit Manager aide du nom de service suivant :

- `com.amazonaws.region.auditmanager`

Si vous activez le DNS privé pour le point de terminaison, vous pouvez envoyer des demandes d'API AWS Audit Manager en utilisant son nom DNS par défaut pour la région, par exemple,`auditmanager.us-east-1.amazonaws.com`.

Pour plus d'informations, consultez Accès à un service via un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Création d'une politique de point de terminaison VPC pour AWS Audit Manager

Vous pouvez attacher une stratégie de point de terminaison à votre point de terminaison d'un VPC qui contrôle l'accès à AWS Audit Manager. La politique spécifie les informations suivantes :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Pour plus d'informations, consultez Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Exemple : politique de point de terminaison VPC pour les actions AWS Audit Manager

Voici un exemple de politique de point de terminaison pour AWS Audit Manager. Lorsqu'elle est associée à un point de terminaison, cette politique accorde l'accès aux actions Audit Manager répertoriées pour tous les principaux sur toutes les ressources.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "auditmanager:GetAssessments",
            "auditmanager:GetServicesInScope",
            "auditmanager:ListNotifications"
         ],
         "Resource":"*"
      }
   ]
}
```

Connexion et surveillance AWS Audit Manager

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Audit Manager et de vos autres AWS solutions. AWS fournit les outils de surveillance

suivants pour surveiller Audit Manager, signaler un problème et prendre des mesures automatiques le cas échéant :

- AWS CloudTrail capture les appels d'API et les événements associés créés par votre Compte AWS ou au nom de celui-ci et livre les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateurAWS CloudTrail.
- Amazon EventBridge est un service de bus d'événements sans serveur qui permet de connecter facilement vos applications à des données provenant de diverses sources. EventBridge fournit un flux de données en temps réel à partir de vos propres applications, applications oftware-as-a S-Service (SaaS) et AWS services et achemine ces données vers des cibles telles que Lambda. Cela vous permet de surveiller les événements qui se produisent dans les services et de créer des architectures basées sur les événements. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.

Surveillance AWS Audit Manager avec Amazon EventBridge

Amazon vous EventBridge aide à automatiser Services AWS et à répondre automatiquement aux événements du système tels que les problèmes de disponibilité des applications ou les modifications des ressources.

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

Par exemple, vous pouvez détecter chaque occurrence des événements suivants d'Audit Manager sur votre compte :

- Le responsable d'audit crée, met à jour ou supprime une évaluation
- Le responsable d'audit délègue une série de contrôles à des fins de révision
- Un délégué termine son examen et renvoie la série de contrôles examiné au responsable d'audit.
- Un responsable d'audit met à jour l'état d'un contrôle d'évaluation

Les actions pouvant être déclenchées automatiquement sont les suivantes :

- Utilisez une AWS Lambda fonction pour transmettre une notification à une chaîne Slack.
- Envoyer les données relatives à la vérification à un Amazon Kinesis Data Streams pour prendre en charge la surveillance complète et en temps réel du statut.
- Envoyer une rubrique Amazon Simple Notification Service (Amazon SNS) à votre e-mail.
- Recevez une notification d'une action CloudWatch d'alarme Amazon.

> **Note**
>
> Audit Manager délivre des événements sur une base durable. Cela signifie qu'Audit Manager tentera avec succès de transmettre des événements EventBridge au moins une fois. Dans les cas où les événements ne peuvent pas être transmis en raison d'une interruption de EventBridge service, ils seront réessayés ultérieurement par l'Audit Manager pendant 24 heures au maximum.

EventBridge exemple de format pour Audit Manager

Le code JSON suivant montre un exemple d'événement de création d'évaluation dans Audit Manager. Pour plus d'informations sur l'un des champs de cet événement, voir Référence de structure d'événement.

```
{
    "version": "0",
    "id": "55c5a6f3-6183-3989-49ec-a3c998857644",
    "detail-type": "Assessment Created",
    "source": "aws.auditmanager",
    "account": "111122223333",
    "time": "2023-07-27T00:38:33Z",
    "region": "us-west-2",
    "resources":
        [
            "arn:aws:auditmanager:us-west-2:111122223333:assessment/a1b2c3d4-e5f6-g7h8-
i9j0-k1l2m3n4o5p6"
        ],
    "detail":
    {
        "eventID": "4e939b2f-9429-3141-beec-d640d83ef68e",
        "author": "arn:aws:sts::111122223333:assumed-role/roleName/role-session-name",
        "assessmentTenantId": "111122223333",
```

```
        "assessmentName": "myAssessment",
        "eventTime": 1690418289068,
        "eventName": "CREATE",
        "eventType": "ASSESSMENT",
        "assessmentID": "a1b2c3d4-e5f6-g7h8-i9j0-k1l2m3n4o5p6"
    }
}
```

Conditions préalables à la création d'une règle EventBridge

Avant de créer des politiques pour les événements Audit Manager, nous vous recommandons de procéder comme suit :

- Familiarisez-vous avec les événements, les règles et les cibles dans EventBridge. Pour plus d'informations, consultez Qu'est-ce qu'Amazon EventBridge ? dans le guide de EventBridge l'utilisateur Amazon.
- Créez la cible à utiliser dans votre règle d'événement. Par exemple, vous pouvez créer une rubrique Amazon SNS, afin de recevoir un texto ou un e-mail à chaque fois que l'examen d'une série de contrôles est terminé. Pour plus d'informations, consultez la section EventBridge Objectifs.

Création d'une EventBridge règle pour Audit Manager

Suivez ces étapes pour créer une EventBridge règle qui se déclenche lors d'un événement émis par Audit Manager. Les événements sont générés dans la mesure du possible.

Pour créer une EventBridge règle pour Audit Manager

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Dans le volet de navigation, choisissez Règles.
3. Choisissez Créer une règle.
4. Sur la page Définir les informations de la règle, saisissez un nom et une description pour la règle.
5. Conservez les valeurs par défaut pour Bus d'événement et Type de règle, puis choisissez Suivant.
6. Sur la page Créer un modèle d'événement, dans Source d'événement, sélectionnez AWS événements ou événements EventBridge partenaires.
7. Dans Méthode de création, choisissez Modèle personnalisé (éditeur JSON).

8. Dans Modèle d'événement, entrez un modèle d'événement au format JSON et spécifiez les champs que vous souhaitez utiliser pour la correspondance.

   Pour faire correspondre un événement Audit Manager, vous pouvez utiliser le modèle simple suivant :

   ```
   {
     "detail-type": ["Event"]
   }
   ```

   Remplacez *Event* par l'une des valeurs prises en charge suivantes :

   a. Saisissez `Assessment Created` pour recevoir des notifications lorsqu'une évaluation est créée.

   b. Saisissez `Assessment Updated` pour recevoir des notifications lorsqu'une évaluation est mise à jour.

   c. Saisissez `Assessment Deleted` pour recevoir des notifications lorsqu'une évaluation est supprimée.

   d. Saisissez `Assessment ControlSet Delegation Created` pour recevoir des notifications lorsqu'une série de contrôles est déléguée pour examen.

   e. Saisissez `Assessment ControlSet Reviewed` pour recevoir des notifications lorsqu'une série de contrôles d'évaluation est examinée.

   f. Saisissez `Assessment Control Reviewed` pour recevoir des notifications lorsqu'un contrôle d'évaluation est examiné.

   > **Tip**
   >
   > Ajoutez d'autres champs à votre modèle d'événement selon vos besoins. Pour plus d'informations sur les champs disponibles, consultez les modèles EventBridge d'événements Amazon.

9. Choisissez Suivant.

10. Sur la page Sélectionner la ou les cibles, choisissez la cible créée pour cette règle, puis configurez toutes les options supplémentaires requises pour ce type. Par exemple, si vous choisissez Amazon SNS, assurez-vous que votre rubrique SNS est configurée correctement pour être notifié par e-mail ou SMS.

> **Tip**
>
> Les champs affichés varient en fonction du service sélectionné. Pour plus d'informations sur les cibles disponibles, consultez la section Cibles disponibles dans la EventBridge console.

11. Pour de nombreux types de cibles, EventBridge nécessite des autorisations pour envoyer des événements à la cible. Dans ces cas, EventBridge vous pouvez créer le rôle IAM nécessaire à l'exécution de votre règle.

    a. Pour créer un rôle IAM automatiquement, sélectionnez Créer un rôle pour cette ressource spécifique.

    b. Pour utiliser un rôle IAM que vous avez créé auparavant, sélectionnez Utiliser un rôle existant.

12. (Facultatif) Sélectionnez Add another target (Ajouter une autre cible) pour ajouter une nouvelle cible pour cette règle.
13. Choisissez Suivant.
14. (Facultatif) Sur la page Configure tags (Configurer des étiquettes), ajoutez des étiquettes, puis choisissez Next (Suivant).
15. Sur la page Vérifier et créer, examinez la configuration de votre règle et assurez-vous qu'elle répond à vos exigences en matière de surveillance d'événements.
16. Choisissez Créer une règle. Votre règle va maintenant surveiller les événements Audit et les envoyer à la cible spécifiée.

Journalisation des appels d' AWS Audit Manager API avec CloudTrail

Audit Manager est intégré à CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS Audit Manager. CloudTrail capture tous les appels d'API pour Audit Manager sous forme d'événements. Les appels capturés incluent les appels de la console Audit Manager et les appels de code vers les opérations d'API d'Audit Manager.

Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Audit Manager. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements.

À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Audit Manager, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite et des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide deAWS CloudTrail l'utilisateur.

Informations sur l'Audit Manager dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans Audit Manager, cette activité est enregistrée dans un CloudTrail événement avec d'autres Service AWS événements dans l'historique des événements.

Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez Affichage des événements avec l'historique des événements CloudTrail .

Pour un enregistrement continu des événements de votre entreprise Compte AWS, y compris des événements pour Audit Manager, créez une trace. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez.

En outre, vous pouvez en configurer d'autres Services AWS pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- CloudTrail Services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions d'Audit Manager sont enregistrées CloudTrail et documentées dans la référence de l'AWS Audit Manager API. Par exemple, les appels aux `CreateCustomControl` opérations `DeleteControl` et `UpdateAssessmentTemplate` API génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec les informations d'identification d'utilisateur root.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

Pour plus d'informations, consultez la section Élément userIdentity CloudTrail .

Comprendre les entrées du fichier journal d'Audit Manager

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`CreateAssessment`action.

```
{
      eventVersion:"1.05",
      userIdentity:{
        type:"IAMUser",
        principalId:"principalId",
        arn:"arn:aws:iam::accountId:user/userName",
        accountId:"111122223333",
        accessKeyId:"accessKeyId",
        userName:"userName",
        sessionContext:{
          sessionIssuer:{
          },
          webIdFederationData:{
          },
          attributes:{
            mfaAuthenticated:"false",
            creationDate:"2020-11-19T07:32:06Z"
          }
        }
```

```
      },
      eventTime:"2020-11-19T07:32:36Z",
      eventSource:"auditmanager.amazonaws.com",
      eventName:"CreateAssessment",
      awsRegion:"us-west-2",
      sourceIPAddress:"sourceIPAddress",
      userAgent:"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
      requestParameters:{
        frameworkId:"frameworkId",
        assessmentReportsDestination:{
          destination:"***",
          destinationType:"S3"
        },
        clientToken:"***",
        scope:{
          awsServices:[
            {
              serviceName:"license-manager"
            }
          ],
          awsAccounts:"***"
        },
        roles:"***",
        name:"***",
        description:"***",
        tags:"***"
      },
      responseElements:{
        assessment:"***"
      },
      requestID:"0d950f8c-5211-40db-8c37-2ed38ffcc894",
      eventID:"a782029a-959e-4549-81df-9f6596775cb0",
      readOnly:false,
      eventType:"AwsApiCall",
      recipientAccountId:"recipientAccountId"
    }
```

Analyse de configuration et de vulnérabilité dans AWS Audit Manager

La configuration et les contrôles informatiques sont une responsabilité partagée entre vous AWS et vous, notre client. Pour plus d'informations, consultez le modèle de responsabilité AWS partagée.

Balisage de ressources AWS Audit Manager

Une balise est une étiquette de métadonnée que vous attribuez ou que AWS attribue à une ressource AWS. Chaque balise se compose d'une clé et d'une valeur. Pour les balises que vous affectez, vous définissez la clé et la valeur. Par exemple, vous pouvez définir la clé sur `stage` et la valeur pour une ressource sur `test`.

Les balises vous permettent d'effectuer les actions suivantes :

- Localisez facilement les ressources de votre Audit Manager. Vous pouvez utiliser des balises comme critères de recherche lorsque vous parcourez la bibliothèque du framework et la bibliothèque de contrôle.
- Associez votre ressource à un type de conformité. Vous pouvez étiqueter plusieurs ressources à l'aide d'une balise spécifique à la conformité afin d'associer ces ressources à un framework spécifique.
- Identifier et organiser vos ressources AWS. De nombreux services Services AWS prennent en charge l'indexation. Vous pouvez donc attribuer le même indexe à des ressources appartenant à différents services, afin d'indiquer que les ressources sont liées.
- Suivre vos coûts AWS. Vous activez ces balises sur le tableau de bord AWS Billing and Cost Management. AWS utilise les balises pour classer vos coûts et pour vous fournir un rapport mensuel d'allocation des coûts. Pour de plus amples informations, veuillez consulter Utilisation des identifications d'allocation des coûts dans le Guide de l'utilisateur AWS Billing and Cost Management.

Les sections suivantes fournissent de plus amples informations sur les balises pour AWS Audit Manager.

Ressources prises en charge dans Audit Manager

Les ressources Audit Manager suivantes prennent en charge le balisage :

- Évaluations
- Contrôles
- Frameworks

Restrictions liées aux balises

Les restrictions de base suivantes s'appliquent aux balises sur les ressources Audit Manager :

- Nombre maximum d'étiquettes que vous pouvez attribuer à une ressource – 50
- Longueur de clé maximale – 128 caractères Unicode
- Longueur de valeur maximale – 256 caractères Unicode
- Caractères valides pour les clés et valeurs – a-z, A-Z, 0-9, espace et les caractères suivants : _ . : / = + - et @
- Les clés et les valeurs sont sensibles à la casse.
- N'utilisez pas `aws:` comme préfixe pour les clés ; seul AWS peut utiliser cette valeur.

Gestion des balises

Vous pouvez définir des balises en tant que propriétés lorsque vous créez une évaluation, un cadre ou un contrôle. Vous pouvez ajouter, modifier et supprimer des balises via la console Audit Manager, le AWS Command Line Interface (AWS CLI) et l'API Audit Manager. Pour de plus amples informations, consultez les liens suivants.

- Pour les évaluations :
  - Création d'une évaluation et Modification d'une évaluation dans la section Évaluations de ce guide
  - Onglet Balises dans la section Vérifier une évaluation de ce guide
  - CreateAssessment et UpdateAssessment dans la référence de l'API AWS Audit Manager
  - TagResource et UntagResource dans le guide de AWS Audit Managerréférence de l'API
- Pour les frameworks :
  - Création d'un framework personnalisé et Modification d'un framework personnalisé dans la section Bibliothèque Framework de ce guide
  - onglet Balises dans la section Afficher les détails du framework de ce guide
  - CreateAssessmentFramework et UpdateAssessmentFramework dans la référence de l'API AWS Audit Manager
  - TagResource et UntagResource dans le guide de AWS Audit Managerréférence de l'API
- Pour les commandes :

- Création d'un contrôle personnalisé et Modification d'un contrôle personnalisé dans la section Bibliothèque de contrôle de ce guide
- onglet Balises dans la section Afficher les détails de contrôle de ce guide
- CreateControl et UpdateControl dans la AWS Audit Manager référence de l'API
- TagResource et UntagResource dans le guide de AWS Audit Managerréférence de l'API

Création de ressources AWS Audit Manager avec AWS CloudFormation

AWS Audit Manager est intégré à AWS CloudFormation, un service qui vous aide à modéliser et à configurer vos ressources AWS afin que vous puissiez consacrer moins de temps à la création et à la gestion de vos ressources et de votre infrastructure. Vous créez un modèle qui décrit toutes les ressources AWS que vous souhaitez utiliser (comme les évaluations), et AWS CloudFormation provisionne et configure ces ressources pour vous.

Lorsque vous utilisez AWS CloudFormation, vous pouvez réutiliser votre modèle pour configurer vos ressources Audit Manager de manière cohérente de nombreuses fois. Décrivez vos ressources une seule fois, puis provisionnez-les autant de fois que vous le souhaitez dans plusieurs comptes et régions AWS.

Audit Manager et modèles AWS CloudFormation

Pour provisionner et configurer des ressources pour Audit Manager et les services associés, vous devez bien comprendre les AWS CloudFormation modèles. Les modèles sont des fichiers texte formatés en JSON ou YAML. Ces modèles décrivent les ressources que vous souhaitez allouer dans vos piles AWS CloudFormation. Si JSON ou YAML ne vous est pas familier, vous pouvez utiliser AWS CloudFormation Designer pour vous aider à démarrer avec des modèles AWS CloudFormation. Pour plus d'informations, consultez Qu'est-ce que AWS CloudFormation Designer ? dans le AWS CloudFormationGuide de l'utilisateur.

Audit Manager prend en charge la création d'évaluations dans AWS CloudFormation. Pour de plus amples informations, y compris des exemples de modèles JSON et YAML pour les évaluations, consultez la rubrique AWS Audit ManagerRéférence du type de ressource dans le Guide de l'utilisateur AWS CloudFormation.

En savoir plus sur AWS CloudFormation

Pour en savoir plus sur AWS CloudFormation, consultez les ressources suivantes :

- AWS CloudFormation
- Guide de l'utilisateur AWS CloudFormation
- Référence API AWS CloudFormation

- Guide de l'utilisateur de l'interface de ligne de commande AWS CloudFormation

Historique du document pour le guide de l'utilisateur des AWS Audit Manager

Le tableau ci-après décrit les modifications importantes dans chaque version du AWS Audit Manager Guide de l'utilisateur à partir du 8 décembre 2020.

Modification	Description	Date
Nouveau framework pris en charge : PCI DSS V4.0	Un nouveau cadre prédéfini est désormais disponible dans AWS Audit Manager. Pour de plus amples informations, consultez la section PCI DSS V4.0.	19 décembre 2023
Support pour les AWS appels d'API supplémentaires	Vous pouvez désormais utiliser des appels d'API AWS supplémentaires comme sources de données pour vos contrôles personnalisés dans Audit Manager. Pour plus d'informations, veuillez consulter la section Appels d'API pris en charge pour les sources de données de contrôles personnalisés.	7 décembre 2023
Politique gérée AWS mise à jour	AWS Audit Manager a mis à jour la AWSAuditManagerServiceRolePolicy. Pour plus d'informations, veuillez consulter AWS politiques gérées pour AWS Audit Manager.	6 décembre 2023

Support pour les AWS Security Hub résultats de contrôle consolidés	Audit Manager prend désormais en charge les contrôles consolidés dans AWS Security Hub. Pour plus d'informations, veuillez consulter AWS Security HubContrôles pris en charge par AWS Audit Manager.	16 novembre 2023
Intégration à MetricStream	Vous pouvez désormais intégrer les preuves d'Audit Manager dans MetricStream. Pour plus d'informations, veuillez consulter Intégrations avec des produits GRC tiers.	14 novembre 2023
Nouveau cadre pris en charge : AWS meilleures pratiques en matière d'IA générative	Un nouveau cadre prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter le AWS cadre des meilleures pratiques en matière d'IA générative v1.	8 novembre 2023
Politique gérée AWS mise à jour	AWS Audit Manager a mis à jour la AWSAuditManagerServiceRolePolicy. Pour plus d'informations, veuillez consulter AWS politiques gérées pour AWS Audit Manager.	6 novembre 2023

Intégration à Amazon EventBridge	Vous pouvez désormais surveiller les événements qui se produisent dans AWS Audit Manager et utiliser ces événements dans le cadre de votre architecture axée sur les événements. Pour plus d'informations, veuillez consulter Surveillance des événements AWS Audit Manager avec Amazon EventBridge.	18 août 2023
Support pour les évaluations des risques et les nouvelles options de preuves manuelles	Vous pouvez désormais utiliser le flux de travail de création de contrôles personnalisés pour appuyer les évaluations des risques. Un contrôle peut désormais représenter une question d'évaluation des risques, et vous pouvez y répondre en téléchargeant un fichier ou en saisissant du texte comme preuve manuelle. Pour plus d'informations, veuillez consulter Création d'un contrôle personnalisé et Ajouter des preuves manuelles .	12 juin 2023

Support pour les exportations au format CSV	Vous pouvez désormais exporter les résultats de votre recherche dans l'outil Evidence finder au format CSV. Pour plus d'informations, veuillez consulter Exporter vos résultats de recherche.	9 juin 2023
Manuel de sécurité de l'information du Centre australien de cybersécurité (Autralian Cyber Security Centre, ACSC)	Un nouveau cadre prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter le manuel de sécurité de l'information du Centre australien de cybersécurité (ACSC).	24 mars 2023
Rapports d'évaluation améliorés	Nous avons amélioré le format et le contenu des rapports d'évaluation d'Audit Manager. Pour plus d'informations sur la navigation et la compréhen sion des rapports d'évaluation, veuillez consulter Rapports d'évaluation.	23 mars 2023
Support pour les appels d'API paginés	AWS Audit Manager prend désormais en charge les appels d'API paginés en tant que source de données pour la collecte de preuves. Pour plus d'informations, veuillez consulter Appels d'API paginés.	8 mars 2023

Nouveau cadre pris en charge : Règle de sécurité omnibus finale HIPAA 2013	Un nouveau cadre prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter la règle de sécurité omnibus finale HIPAA 2013. À des fins de différenciation, le cadre HIPAA existant (ancienne ment nommé HIPAA dans la bibliothèque de cadres) s'appelle désormais Règle de sécurité HIPAA 2003.	8 mars 2023
Support pour les AWS appels d'API supplémentaires	Vous pouvez désormais utiliser neuf AWSappels d'API supplémentaires comme source de données pour vos contrôles personnalisés dans Audit Manager. Pour plus d'informations, veuillez consulter la section Appels d'API pris en charge pour les sources de données de contrôles personnalisés.	3 mars 2023
Guide mis à jour pour s'aligner sur les bonnes pratiques IAM	Guide mis à jour pour s'aligner sur les bonnes pratiques IAM. Pour de plus amples informati ons, veuillez consulter Bonnes pratiques de sécurité dans IAM.	6 janvier 2023

Nouveau paramètre de conservation des données	Vous pouvez désormais spécifier si vous souhaitez supprimer toutes vos données lorsque vous désactivez Audit Manager. Pour plus d'informations, veuillez consulter la section Désactivation AWS Audit Manager et Suppression des données d'Audit Manager.	6 janvier 2023
Support pour Evidence Finder	Vous pouvez désormais utiliser l'outil de recherche de preuves pour effectuer des recherches sur vos données de preuves. Pour plus d'informations, veuillez consulter Evidence finder.	18 novembre 2022
Nouveau cadre pris en charge : Essential Eight du Centre australien de cybersécurité (ACSC)	Un nouveau cadre prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter Australian Cyber Security Centre (ACSC) Essential Eight.	24 août 2022
Politique gérée AWS mise à jour	AWS Audit Manager a mis à jour la AWSAuditManagerServiceRolePolicy. Pour plus d'informations, veuillez consulter AWS politiques gérées pour AWS Audit Manager.	7 juillet 2022

Politique gérée AWS mise à jour	AWS Audit Manager a mis à jour la AWSAuditManagerServiceRolePolicy. Pour plus d'informations, veuillez consulter AWS politiques gérées pour AWS Audit Manager.	20 mai 2022
Nouveau cadre pris en charge : Profil de contrôle du cloud de taille moyenne du Centre canadien pour la cybersécurité	Un nouveau cadre prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter le profil de contrôle du cloud de taille moyenne du Centre canadien pour la cybersécurité.	6 mai 2022
Politique gérée AWS mise à jour	AWS Audit Manager a mis à jour la politique AWSAuditManagerAdministratorAccess. Pour plus d'informations, veuillez consulter AWS politiques gérées pour AWS Audit Manager.	29 avril 2022
Support pour des règles gérées AWS Config supplémentaires	Vous pouvez désormais utiliser 91 règles gérées AWS Config supplémentaires comme source de données pour vos contrôles personnalisés dans Audit Manager. Pour plus d'informations, veuillez consulter la section Utilisation de règles gérées AWS Config avec AWS Audit Manager.	27 avril 2022

Support pour les règles personnalisées AWS Config	Vous pouvez désormais utiliser des règles personnalisées AWS Config comme source de données pour vos contrôles personnalisés dans Audit Manager. Pour plus d'informations, veuillez consulter la section Utilisation de règles AWS Config personnalisées avec AWS Audit Manager.	27 avril 2022
Nouveau cadre pris en charge : ISO/IEC 27001:2013 Annexe A	Un nouveau cadre prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter l'annexe A de la norme ISO/IEC 27001:2013.	7 avril 2022
Politique gérée AWS mise à jour	AWS Audit Manager a mis à jour la AWSAuditManagerServiceRolePolicy. Pour plus d'informations, veuillez consulter AWS politiques gérées pour AWS Audit Manager.	16 mars 2022

Nouveaux cadres pris en charge : CIS Benchmark pour CIS Amazon Web Services Foundations Benchmark v1.4	Deux nouveaux cadres prédéfinis sont désormais disponibles dans AWS Audit Manager : CIS Benchmark pour CIS Amazon Web Services Foundations Benchmark v1.4, Niveau 1, et CIS Benchmark pour CIS Amazon Web Services Foundations Benchmark v1.4, Niveaux 1 et 2. Pour plus d'informations, veuillez consulter CIS Benchmark pour CIS AWS Audit Manager Foundations Benchmark v1.4.0.	2 mars 2022
Nouveau cadre pris en charge : CIS Controls v8 IG1	Un nouveau cadre prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter CIS Controls v8 IG1.	2 mars 2022
Tableau de bord AWS Audit Manager	Vous pouvez désormais utiliser le tableau de bord d'Audit Manager pour surveille r vos évaluations actives et identifier rapidement les preuves non conformes. Pour plus d'informations, veuillez consulter Utiliser le tableau de bord d'Audit Manager.	18 novembre 2021

Partage d'un framework personnalisé	Vous pouvez désormais partager vos cadres Audit Manager personnalisés avec un autre Compte AWS, ou les répliquer dans un autre Région AWS sous votre propre compte. Pour plus d'informations, veuillez consulter Partage d'un cadre personnalisé.	22 octobre 2021
Nouveaux exemples de contrôles AWS Audit Manager	Vous pouvez désormais consulter des exemples de contrôles et découvrir comment Audit Manager contribue à adapter votre environnement AWS à leurs exigences. Pour plus d'informations, veuillez consulter la section Exemples de contrôles AWS Audit Manager.	21 septembre 2021
Nouveau cadre pris en charge : Loi Gramm-Leach-Bliley (GLBA)	Un nouveau cadre prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter la Loi Gramm-Leach-Bliley (GLBA).	2 septembre 2021
Nouveau chapitre Résolution des problèmes	Un nouveau chapitre Résolution des problèmes est désormais disponible. Pour plus d'informations, veuillez consulter Résolution des problèmes dans AWS Audit Manager.	23 août 2021

Nouveau chapitre et tutoriel sur la délégation	Nous avons élargi notre documentation de délégation dans un nouveau chapitre. Pour plus d'informations, veuillez consulter Délégations dans AWS Audit Manager. Nous avons également ajouté un nouveau tutoriel destiné aux délégués qui examinent un ensemble de contrôles pour la première fois depuis AWS Audit Manager. Pour plus d'informations, veuillez consulter Tutoriel pour les délégués : Révision d'un ensemble de contrôles.	25 juin 2021
Nouveau cadre pris en charge : NIST SP 800-171 Rev. 2	Un nouveau cadre prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter NIST SP 800-171 Rev. 2.	17 juin 2021
Rapports d'évaluation améliorés	Nous avons amélioré le format et le contenu des rapports d'évaluationAWS Audit Manager. Pour plus d'informations sur la façon de naviguer dans les nouveaux rapports d'évaluation et de les comprendre, veuillez consulter la section Rapports d'évaluation.	8 juin 2021

Nouvelle AWS Page de politiques gérées	AWS Audit Manager a commencé à suivre les modifications pour ses politiques gérées. Pour plus d'informations, veuillez consulter Politiques gérées AWS pour AWS Audit Manager.	6 mai 2021
Nouveau cadre pris en charge : Cadre de cybersécurité du NIST version 1.1	Un nouveau cadre prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter la version 1.1 du cadre de cybersécurité du NIST.	5 mai 2021
Nouveau cadre pris en charge : AWS Bien architecturé	Un nouveau cadre prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter AWS Bien architecturé.	5 mai 2021
Nouveau cadre pris en charge : AWS Bonnes pratiques de sécurité de base	Un nouveau cadre prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter AWS Bonnes pratiques de sécurité de base.	5 mai 2021
Nouveau cadre pris en charge : GxP UE Annexe 11	Un nouveau cadre prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter Annexe 11 de la GxP UE.	28 avril 2021

Nouveau cadre pris en charge : NIST 800-53 (Rév. 5) Faible-modéré-élevé	Un nouveau cadre prédéfini est désormais disponible dans AWS Audit Manager. Pour plus d'informations, veuillez consulter NIST 800-53 (Rév. 5) Faible-modéré-élevé.	25 mars 2021
Nouveaux cadres pris en charge : CIS Benchmark pour CIS AWS Audit Manager Foundations Benchmark v1.3	Deux nouveaux cadres prédéfinis sont désormais disponibles dans AWS Audit Manager : CIS Benchmark pour CIS AWS Audit Manager Foundations Benchmark v1.3.0, Niveau 1, et CIS Benchmark pour CIS AWS Audit Manager Foundations Benchmark v1.3.0, Niveaux 1 et 2. Pour plus d'informations, veuillez consulter CIS Benchmark pour CIS AWS Audit Manager Foundations Benchmark v1.3.0.	22 mars 2021
Première version	Première version du Guide de l'utilisateur et référence de l'API AWS Audit Manager.	8 décembre 2020

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le Glossaire AWS dans la Référence Glossaire AWS.

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.