Concepts et procédures AMS Accelerate

Guide de l'utilisateur d'AMS Accelerate

Version October 3, 2025

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Guide de l'utilisateur d'AMS Accelerate: Concepts et procédures AMS Accelerate

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d'Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d'une manière susceptible d'entraîner une confusion chez les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon sont la propriété de leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce qu'AMS Accelerate ? 1
Plans d'opérations 1
Accélérez le plan des opérations 2
Plan d'opérations avancé 2
Fonctionnement 3
Termes clés 3
Service description (Description du service) 10
Fonctionnalités du plan d'exploitation AWS Managed Services (AMS) AMS Accelerate 10
Configurations prises en charge 14
Services pris en charge 16
Rôles et responsabilités 20
Étendue des modifications effectuées par AMS Accelerate 35
Systèmes d'exploitation non pris en charge 36
Contact et escalade 37
Heures de contact 38
Heures d'ouverture 39
Voie d'escalade 39
Inventaire des ressources 40
Mise en route 41
Intégration 41
Conditions préalables à l’onboarding 41
Étape 1. Découverte du compte 44
Étape 2. Ressources de gestion de l'intégration 46
Étape 3. Fonctionnalités d'intégration avec politiques par défaut 56
Étape 4 : Personnalisez les fonctionnalités 67
Utilisation des consoles AMS 69
Motifs AMS 71
Comment fonctionnent les modèles AMS 71
Motifs AMS 72
Configuration d'instance automatisée 76
Fonctionnement 77
Installation automatique de l'agent SSM 78
Modifications de configuration d'instance automatisées 80
Déconnecter d'AMS Accelerate 84

Effets d'offboarding 85
Débarquement avec dépendances 87
Obtenir une assistance pour le débarquement 88
Paramètres de notification 88
Identification 90
Balises 91
Qu'est-ce qu'une balise ? 92
Comment fonctionne le balisage 92
Tags gérés par le client 92
Accélérez la gestion des balises 96
Balises fournies par le client 97
Outils de gestion des balises 98
Étiqueteur de ressources 98
CloudFormation 119
Terraform 123
Rapports d'incidents, demandes de service et questions de facturation 125
Gestion des incidents 125
Qu'est-ce que la gestion des incidents ? 126
Comment fonctionnent la réponse et la résolution des incidents 127
Gérer les incidents 128
Gestion des demandes de service 131
Quand utiliser une demande de service 133
Comment fonctionne la gestion des demandes de service 133
Création d'une demande de service 134
Surveillance et mise à jour d'une demande de service 135
Gestion des demandes de service avec l'API de support 137
Répondre à une demande de service générée par AMS Accelerate 137
Rapport d'incident et test des demandes de service 138
Questions relatives à la facturation 138
Gestion des événements planifiés 139
Critères AMS PEM 139
Types de PEM 139
Le processus AMS PEM 140
PEM FAQs 140
Opérations à la demande 142
Demande d'opérations AMS à la demande 152

Apporter des modifications aux offres d'opérations à la demande 153
Rapports et options 154
Rapports sur demande 154
Rapports de gestion des hôtes AMS 155
Rapports AMS Backup 155
AWS Config Rapport de conformité des contrôles 158
Rapport de configuration des réponses aux règles de configuration AMS Config 160
Incidents évités et suivi des rapports Top Talkers 162
Rapport détaillé sur les frais de facturation 164
Rapports Trusted Remediator 165
Rapports en libre-service 168
Opérations internes de l'API 170
Rapport de patch (quotidien) 173
Rapport de sauvegarde (quotidien) 183
Rapport d'incident (hebdomadaire) 188
Rapport de facturation (mensuel) 191
Rapports agrégés 194
Tableaux de bord de rapports en libre-service AMS 196
Stratégie de conservation des données 204
Débarquer de la SSR 205
Gestion de l'accès 206
Accès à la console 206
Autorisations d'utilisation des fonctionnalités 206
Pourquoi et quand accédons-nous à votre compte 221
déclencheurs d'accès 221
Accéder aux rôles IAM 222
Comment accédons-nous à votre compte 224
Comment et quand utiliser root 225
Gestion de la sécurité 226
Utilisation du document Log4j SSM pour découvrir des occurrences 227
Surveillance de la sécurité de l'infrastructure 228
Utilisation des rôles liés à un service 230
AWS politiques gérées 243
Protection des données 252
Surveillez avec Amazon Macie 253
Moniteur avec GuardDuty 253

Surveillez avec le pare-feu DNS Amazon Route 53 Resolver 255
Chiffrement des données 257
AWS Identity and Access Management 257
Authentification avec des identités dans AMS Accelerate 257
Gestion des accès à l’aide de politiques 265
Réponse aux incidents de sécurité 266
Fonctionnement 267
Préparation 268
Détection 269
Analyser 269
Contenir 271
Éradiquer 273
Récupération 273
Rapport post-incident 274
Runbooks de réponse aux incidents de sécurité 275
Enregistrement et surveillance des événements de sécurité 281
Conformité de la configuration 281
Bibliothèque de règles de configuration AMS 282
Réponses aux violations 307
Création d'exceptions aux règles 309
Réduisez AWS Config les coûts 310
Constatations et réponses personnalisées 310
Intervention en cas d’incidents 313
Réponse aux incidents et intégration 313
Résilience 313
Contrôle de sécurité pour les systèmes end-of-support d'exploitation 314
Bonnes pratiques de sécurité 314
Examens de sécurité des demandes de modification 315
Processus de gestion des risques liés à la sécurité des clients 315
Normes techniques AMS Accelerate 316
Commandes standard dans AMS Accelerate 316
Changements qui introduisent des risques de sécurité élevés ou très élevés dans votre environnement 332
FAQ sur la sécurité 334
Quand les ingénieurs opérationnels d'AMS accèdent-ils à mes environnements ? 334

Quels sont les rôles des ingénieurs d'exploitation AMS lorsqu'ils accèdent à mes comptes ? 335
Comment un ingénieur des opérations AMS accède-t-il à mon compte ? 335
Comment suivre les modifications apportées par AMS dans mes AWS comptes gérés par AMS ? 336
Quels sont les contrôles de processus permettant à l'ingénieur des opérations AMS d'accéder à mon compte ? 337
Comment sont gérés les accès privilégiés ? 337
Les ingénieurs d'exploitation d'AMS utilisent-ils le MFA ? 337
Qu'advient-il de leur accès lorsqu'un employé d'AMS quitte l'organisation ou change de rôle ? 337
Quels contrôles d'accès régissent l'accès des ingénieurs d'exploitation AMS à mes comptes ? 337
Comment AMS surveille-t-il l'accès des utilisateurs root ? 338
Comment l'AMS réagit-il aux incidents de sécurité ? 338
Quels sont les cadres et certifications standard du secteur auxquels AMS adhère ? 339
Comment puis-je accéder aux derniers rapports sur la certification de sécurité, les cadres et la conformité AWS ? 339
AMS partage-t-il des diagrammes d'architecture de référence illustrant les différents aspects des fonctionnalités d'AMS ? 340
Comment AMS vérifie-t-elle qui accède à mes comptes et quels sont les besoins de l'entreprise en matière d'accès ? 340
Les ingénieurs d'AMS ont-ils accès à mes données stockées dans un service de stockage de AWS données, tel qu'Amazon S3, Amazon RDS, DynamoDB et Amazon Redshift ? 341
Les ingénieurs d'AMS ont-ils accès aux données clients stockées dans Amazon EBS, Amazon EFS et Amazon FSx ? 341
Comment l'accès est-il restreint ou contrôlé pour les rôles d'automatisation dotés de privilèges élevés pour mes environnements ? 341
Comment AMS met-il en œuvre le principe du moindre privilège tel que préconisé dans le AWS Well-Architected Framework pour les rôles d'automatisation ? 342
Quels sont les systèmes de journalisation et de surveillance utilisés pour détecter les tentatives d'accès non autorisées ou les activités suspectes impliquant des rôles d'automatisation ? 342
Comment sont gérés les incidents ou violations de sécurité concernant l'infrastructure d'automatisation, et quels protocoles contribuent à une réponse et à une atténuation rapides ? 342

Des évaluations de sécurité, des analyses de vulnérabilité et des tests de pénétration sont-ils régulièrement effectués sur l'infrastructure d'automatisation ? ... 343
Comment l'accès à l'infrastructure d'automatisation est-il limité au personnel autorisé uniquement ? ... 343
Quelles sont les mesures mises en œuvre pour respecter les normes de sécurité et empêcher les accès non autorisés ou les violations de données dans le pipeline d'automatisation ? ... 343
La détection ou la surveillance des anomalies sont-elles activées pour les accès ou la journalisation des audits pour détecter l'augmentation des privilèges ou les abus d'accès afin d'alerter de manière proactive l'équipe AMS ? ... 344
Quels types de données clients sont extraits des comptes gérés par AMS, et comment sont-ils utilisés et stockés ? ... 344
Surveillance et gestion des événements ... 346
Qu'est-ce que le monitoring ? ... 347
Fonctionnement de la surveillance ... 348
EC2 notifications groupées par instances ... 349
Notification d'alerte basée sur des balises ... 350
Alertes issues de la surveillance de base dans AMS ... 351
Notifications d'incidents liées aux applications dans AMS ... 376
Intégrez AppRegistry et créez des applications ... 377
Créez des balises pour permettre l'enrichissement des dossiers ... 378
Personnalisez la gravité des demandes de support AMS en fonction de vos applications ... 378
Vérifiez les autorisations requises ... 379
Gestionnaire d'alarmes ... 380
Comment fonctionne Alarm Manager ... 380
Commencer à utiliser Alarm Manager ... 382
Balises Alarm Manager ... 382
Profils de configuration d'Alarm Manager ... 387
Création d' CloudWatch alarmes supplémentaires ... 406
Afficher le nombre de ressources surveillées par Alarm Manager ... 406
Correction automatique des alertes par AMS ... 408
EC2 échec de la vérification de l'état : notes sur l'automatisation des mesures correctives ... 413
EC2 automatisation de la correction de l'utilisation des volumes ... 414
Automatisation de la correction des événements liés à un faible niveau de stockage sur Amazon RDS ... 415
Routeur d'événements AMS ... 415

Amazon EventBridge Managed Rules déployées par AMS 416
Création de règles gérées pour AMS 419
Modification des règles gérées pour AMS 419
Suppression de règles gérées pour AMS 419
Correcteur fiable 419
Principaux avantages 419
Comment fonctionne Trusted Remediator 420
Termes clés 421
Commencez avec Trusted Remediator 422
Recommandations de Compute Optimizer prises en charge 425
Trusted Advisor Chèques pris en charge 430
Configuration de la correction des chèques 490
Flux de décision concernant le mode d'exécution 494
Configurer les didacticiels de correction 495
Travailler avec des mesures correctives 498
Journaux de correction 502
Intégration avec QuickSight 507
Bonnes pratiques 509
FAQs 510
Surveillance et gestion des incidents pour EKS 514
Qu'est-ce que la surveillance et la gestion des incidents pour Amazon EKS ? 514
Fonctionnement de la surveillance et de la gestion des incidents pour Amazon EKS 515
Matrice de responsabilité AMS (RACI) 516
Alertes de base 518
Alertes et actions 519
Prérequis 527
Intégration 529
Hors bord 530
Gestion de la continuité 532
Comment fonctionne la gestion de la continuité 532
Sélectionnez un plan de sauvegarde AMS 533
Plan de sauvegarde AMS par défaut 534
Plan de sauvegarde amélioré 534
Plan de sauvegarde sensible aux données 535
Plan de sauvegarde pour l'intégration d'AMS Accelerate 535
Marquez vos ressources pour les sauvegarder 536

Afficher les sauvegardes dans les coffres-forts AMS ... 538
Surveillance et génération de rapports pour les sauvegardes ... 539
Gestion des correctifs ... 541
Recommandations relatives aux correctifs ... 542
Recommandations relatives à la responsabilité des correctifs ... 543
Conseils pour les équipes de candidature ... 544
Conseils pour les équipes chargées des opérations de sécurité ... 545
Conseils pour les équipes de gouvernance et de conformité ... 545
Exemple de conception pour une application Windows à haute disponibilité ... 545
Recommandations relatives aux correctifs FAQs ... 546
Création d'une fenêtre de correctifs ... 547
Limites des fenêtres de maintenance des correctifs ... 547
Créer une fenêtre de patch Patch Tuesday : console AMS ... 548
Créer une fenêtre de correctif : AWS CloudFormation ... 550
Création d'une fenêtre de correctifs : console Systems Manager ... 551
Créer une fenêtre de correctif : Systems Manager CLI ... 553
Patch avec crochets ... 554
Crochets de raccordement AMS RACI ... 554
Création de documents SSM pour les patchhooks ... 556
Configurez la fenêtre de maintenance des correctifs AMS pour utiliser vos documents de commande SSM comme patch-hooks AMS ... 556
Base de référence des correctifs AMS Accelerate ... 558
Ligne de base de correctifs par défaut ... 558
Base de référence personnalisée pour les correctifs ... 559
Autorisations d'application de correctifs à la demande ... 559
Comprendre les notifications relatives aux correctifs et les défaillances des correctifs ... 561
Demandes de service de correctifs et notifications par e-mail ... 561
Notifications de correctifs via CloudWatch des événements ... 562
Enquête sur les défaillances des correctifs ... 566
Optimisation des coûts avec AMS Resource Scheduler ... 567
Utilisation des ressources avec le planificateur de ressources ... 568
Planificateur de ressources d'intégration ... 570
Personnalisation du planificateur de ressources ... 570
Utilisation du planificateur de ressources ... 571
Travailler avec les périodes et les horaires ... 574
Balisage des ressources ... 580

Estimateur de coûts 581
Suppresseur d'alarme 582
Gestion des journaux 583
Gestion des journaux — AWS CloudTrail 583
Accès aux CloudTrail journaux et audit 585
Protection et conservation CloudTrail des journaux 585
Accès aux EC2 journaux Amazon 585
Conservation des EC2 journaux Amazon 586
Gestion des journaux — Amazon EC2 586
Gestion des journaux — Amazon VPC Flow Logs 587
Suivi des modifications 589
Afficher vos enregistrements de modifications 590
Requêtes par défaut 591
Modification du filtre date/heure dans les requêtes 600
Exemples de requêtes par défaut 601
Modifier les autorisations d'enregistrement 612
AWS Systems Manager dans Accelerate 614
Documents AMS Accelerate SSM disponibles 614
Versions des documents AMS Accelerate SSM 615
Tarification Systems Manager 615
Historique de la documentation 616
Mises à jour antérieures 638
..... dclxvii

Qu'est-ce qu'AMS Accelerate ?

Bienvenue sur AMS Accelerate pour Amazon Web Services (AWS). AMS Accelerate fournit une gamme de services opérationnels pour vous aider à atteindre l'excellence opérationnelle sur AWS. Que vous débutiez dans le cloud, que vous cherchiez à renforcer votre équipe actuelle ou que vous ayez besoin d'une solution opérationnelle à long terme, Accelerate peut vous aider à atteindre vos objectifs opérationnels dans le cloud. En nous appuyant sur Services AWS une bibliothèque d'automatisations, de configurations et de manuels d'exécution, nous proposons une solution end-to-end opérationnelle pour les environnements nouveaux et existants AWS .

Le service Accelerate s'appuie sur une suite de fonctionnalités natives Services AWS pour fournir un ensemble complet de fonctionnalités de gestion de l'infrastructure. Dans ce cadre Services AWS, Accelerate crée et gère des ensembles sélectionnés de contrôles de surveillance, de garde-fous de détection, d'automatisations et de runbooks pour exploiter l'infrastructure de manière conforme et sécurisée.

Rubriques

- Plans d'opérations AMS
- Utilisation du plan d'exploitation AMS Accelerate
- Termes clés d'AMS
- Service description (Description du service)
- Fonctionnalités pour les systèmes d'exploitation non pris en charge dans Accelerate
- Contact et escalade
- Inventaire des ressources pour Accelerate

Plans d'opérations AMS

AWS Managed Services (AMS) est disponible avec deux plans d'exploitation : AMS Accelerate et AMS Advanced. Un plan d'exploitation propose un ensemble spécifique de fonctionnalités et comporte différents niveaux de service, de capacités techniques, d'exigences, de prix et de restrictions. Nos plans d'exploitation vous offrent la flexibilité de sélectionner les capacités opérationnelles adaptées à chacune de vos charges de AWS travail. Cette section décrit les fonctionnalités et les différences, ainsi que les responsabilités, les fonctionnalités et les avantages associés à chaque plan, afin que vous puissiez comprendre quel plan d'exploitation convient le mieux à vos comptes.

Pour une comparaison détaillée des fonctionnalités des deux plans d'exploitation, consultez AWS Managed Services Features.

Plan d'opérations AMS Accelerate

AMS Accelerate est le plan d'exploitation AMS qui vous aide à gérer l' day-to-dayinfrastructure de votre AWS environnement nouveau ou existant. AMS Accelerate fournit des services opérationnels, tels que la surveillance, la gestion des incidents et la sécurité. AMS Accelerate propose également un module complémentaire de correctif en option pour les charges de travail EC2 basées sur Amazon qui nécessitent des correctifs réguliers.

Avec AMS Accelerate, vous décidez laquelle Comptes AWS vous souhaitez qu'AMS Accelerate fonctionne, les régions AWS dans lesquelles vous souhaitez qu'AMS Accelerate fonctionne, les modules complémentaires dont vous avez besoin et les contrats de niveau de service (SLAs) dont vous avez besoin. Pour plus de détails, consultez la section Utilisation du plan d'exploitation AMS Accelerate et la description du service.

Plan d'opérations AMS Advanced

AMS Advanced fournit des services de cycle de vie complets pour fournir, exécuter et soutenir votre infrastructure. Outre les services opérationnels fournis par AMS Accelerate, AMS Advanced inclut également des services supplémentaires, tels que la gestion des zones d'atterrissage, les modifications et le provisionnement de l'infrastructure, la gestion des accès et la sécurité des terminaux.

AMS Advanced déploie une zone de landing zone vers laquelle vous migrez vos AWS charges de travail et recevez les services opérationnels AMS. Nos zones d'accueil multi-comptes gérées sont préconfigurées avec l'infrastructure nécessaire pour faciliter l'authentification, la sécurité, la mise en réseau et la journalisation.

AMS Advanced inclut également un système de gestion des modifications et des accès qui protège vos charges de travail en empêchant les accès non autorisés ou la mise en œuvre de modifications risquées dans votre AWS infrastructure. Les clients doivent créer une demande de modification (RFC) à l'aide de notre système de gestion des modifications pour implémenter la plupart des modifications dans leurs comptes AMS Advanced. Vous créez RFCs à partir d'une bibliothèque de modifications automatisées préalablement approuvées par nos équipes de sécurité et d'exploitation ou vous demandez des modifications manuelles qui sont examinées et mises en œuvre par notre équipe des opérations si elles sont considérées à la fois sûres et prises en charge par AMS Advanced.

Utilisation du plan d'exploitation AMS Accelerate

AMS Accelerate est le plan d'exploitation AMS qui permet d'exploiter l'infrastructure AWS supportant les charges de travail. Que vos charges de travail soient déjà enregistrées dans un compte AWS ou que vous envisagiez d'en migrer de nouveaux, vous pouvez bénéficier des services opérationnels d'AMS Accelerate tels que la surveillance et les alertes, la gestion des incidents, la gestion de la sécurité et la gestion des sauvegardes, sans avoir à effectuer une nouvelle migration, à subir des interruptions de service ou à modifier la façon dont vous utilisez AWS. AMS Accelerate propose également un module complémentaire de correctif en option pour les charges de travail EC2 basées nécessitant des correctifs réguliers.

Avec AMS Accelerate, vous avez la liberté d'utiliser, de configurer et de déployer tous les services AWS de manière native ou avec vos outils préférés. Vous pouvez continuer à utiliser vos mécanismes d'accès et de modification existants, tandis qu'AMS applique constamment des pratiques éprouvées qui permettent de développer votre équipe, d'optimiser les coûts, d'accroître la sécurité et l'efficacité et d'améliorer la résilience.

Bien qu'AMS Accelerate puisse simplifier vos opérations, vous restez responsable du développement, du déploiement, du test, du réglage et de la gestion des applications. AMS Accelerate apporte des modifications à votre compte uniquement à la suite d'incidents, d'alarmes, de mesures correctives et de certaines demandes de service. AMS Accelerate ne fournit pas de ressources sur le compte en votre nom. AMS Accelerate fournit une assistance pour le dépannage des problèmes d'infrastructure qui ont un impact sur les applications, mais AMS Accelerate n'accède pas aux configurations de vos applications et ne les valide pas à votre insu et sans votre approbation. Les services et les modifications d'AMS Accelerate sont fournis directement dans la AWS console APIs, ce qui vous permet de continuer à tirer parti de vos comptes existants AWS et des solutions AWS Marketplace disponibles. AMS Accelerate ne modifie pas le code de vos infrastructure-as-code modèles (par exemple, les AWS CloudFormation modèles), mais peut indiquer à vos équipes quelles modifications sont nécessaires pour suivre les meilleures pratiques opérationnelles et de sécurité.

Termes clés d'AMS

- AMS Advanced : les services décrits dans la section « Description du service » de la documentation avancée d'AMS. Voir la description du service.
- Comptes AMS Advanced : AWS comptes qui répondent à tout moment à toutes les exigences des exigences d'intégration avancées d'AMS. Pour plus d'informations sur les avantages d'AMS

Advanced, pour des études de cas et pour contacter un commercial, consultez AWS Managed Services.

- Comptes AMS Accelerate : AWS comptes qui répondent à tout moment à toutes les exigences des exigences d'intégration d'AMS Accelerate. Consultez la section Mise en route avec AMS Accelerate.
- AWS Managed Services : AMS et/ou AMS Accelerate.
- Comptes AWS Managed Services : les comptes AMS et/ou les comptes AMS Accelerate.
- Recommandation critique : Recommandation émise par le AWS biais d'une demande de service vous informant que votre action est nécessaire pour vous protéger contre les risques potentiels ou les perturbations affectant vos ressources ou le Services AWS. Si vous décidez de ne pas suivre une recommandation critique à la date spécifiée, vous êtes seul responsable de tout préjudice résultant de votre décision.
- Configuration demandée par le client : tout logiciel, service ou autre configuration qui n'est pas identifié dans :
  - Accélérer : configurations prises en charge ou AMS Accelerate ; description du service.
  - AMS Advanced : configurations prises en charge ou AMS Advanced ; description du service.
- Communication en cas d'incident : AMS vous communique un incident ou vous demandez un incident avec AMS via un incident créé dans le Centre de support pour AMS Accelerate et dans la console AMS pour AMS. La console AMS Accelerate fournit un résumé des incidents et des demandes de service sur le tableau de bord et des liens vers le centre de support pour plus de détails.
- Environnement géré : les comptes AMS Advanced et/ou les comptes AMS Accelerate gérés par AMS.

  Pour AMS Advanced, cela inclut les comptes de zone d'atterrissage à comptes multiples (MALZ) et de zone d'atterrissage à compte unique (SALZ).
- Date de début de facturation : le jour ouvrable suivant la AWS réception des informations demandées dans l'e-mail d'accueil d'AWS Managed Services. L'e-mail d'intégration d'AWS Managed Services fait référence à l'e-mail que vous avez envoyé pour collecter les informations nécessaires à l'activation d'AWS Managed Services sur vos comptes. AWS

  Pour les comptes que vous avez inscrits ultérieurement, la date de début de facturation est le jour suivant l'envoi par AWS Managed Services d'une notification d'activation d'AWS Managed Services pour le compte inscrit. Une notification d'activation d'AWS Managed Services se produit lorsque :

1. Vous accordez l'accès à un AWS compte compatible et vous le transmettez à AWS Managed Services.
2. AWS Managed Services conçoit et crée le compte AWS Managed Services.

- Résiliation du service : vous pouvez résilier les services AWS Managed Services pour tous les comptes AWS Managed Services, ou pour un compte AWS Managed Services spécifique pour quelque raison que ce soit, en fournissant un préavis d' AWS au moins 30 jours par le biais d'une demande de service. À la date de fin du service, soit :
  1. AWS vous confie le contrôle de tous les comptes AWS Managed Services ou des comptes AWS Managed Services spécifiés, selon le cas, ou
  2. Les parties suppriment les AWS Identity and Access Management rôles donnant AWS accès à tous les comptes AWS Managed Services ou aux comptes AWS Managed Services spécifiés, selon le cas.
- Date de fin du service : La date de fin du service est le dernier jour du mois civil suivant la fin de la période de préavis de résiliation requise de 30 jours. Si la fin de la période de préavis de résiliation requise tombe après le 20e jour du mois civil, la date de fin du service est le dernier jour du mois civil suivant. Voici des exemples de scénarios relatifs aux dates de résiliation.
  - Si l'avis de résiliation est fourni le 12 avril, le préavis de 30 jours prend fin le 12 mai. La date de fin du service est le 31 mai.
  - Si un préavis de résiliation est fourni le 29 avril, le préavis de 30 jours prend fin le 29 mai. La date de fin du service est le 30 juin.
- Fourniture d'AWS Managed Services : AWS met à votre disposition et vous pouvez accéder à AWS Managed Services et les utiliser pour chaque compte AWS Managed Services à compter de la date de début du service.
- Résiliation de comptes AWS Managed Services spécifiques : vous pouvez résilier les services AWS Managed Services pour un compte AWS Managed Services spécifique pour quelque raison que ce soit en fournissant un AWS préavis par le biais d'une demande de service (« Demande de résiliation de compte AMS »).

Termes de gestion des incidents :

- Événement : modification de votre environnement AMS.
- Alerte : chaque fois qu'un événement provenant d'un Service AWS service pris en charge dépasse un seuil et déclenche une alarme, une alerte est créée et une notification est envoyée à votre liste de contacts. En outre, un incident est créé dans votre liste d'incidents.

- Incident : interruption imprévue ou dégradation des performances de votre environnement AMS ou d'AWS Managed Services ayant un impact tel que signalé par AWS Managed Services ou par vous-même.
- Problème : cause sous-jacente partagée d'un ou de plusieurs incidents.
- Résolution d'un incident ou résolution d'un incident :
  - AMS a rétabli tous les services ou ressources AMS indisponibles relatifs à cet incident à un état disponible, ou
  - AMS a déterminé que les piles ou les ressources indisponibles ne peuvent pas être restaurées à un état disponible, ou
  - AMS a lancé une restauration de l'infrastructure que vous avez autorisée.
- Temps de réponse aux incidents : différence de temps entre le moment où vous créez un incident et le moment où AMS fournit une réponse initiale par le biais de la console, du courrier électronique, du centre de service ou du téléphone.
- Temps de résolution de l'incident : différence de temps entre le moment où AMS ou vous-même créez un incident et le moment où l'incident est résolu.
- Priorité des incidents : comment les incidents sont classés par ordre de priorité par AMS, ou par vous, comme étant faible, moyen ou élevé.
  - Faible : problème non critique lié à votre service AMS.
  - Moyen : au sein de votre environnement géré, un service AWS est disponible mais ne fonctionne pas comme prévu (conformément à la description du service applicable).
  - Élevé : soit (1) la console AMS, soit un ou plusieurs AMS de APIs votre environnement géré ne sont pas disponibles ; soit (2) une ou plusieurs piles ou ressources AMS de votre environnement géré ne sont pas disponibles et cette indisponibilité empêche votre application de fonctionner correctement.

  AMS peut reclasser les incidents conformément aux directives ci-dessus.
- Restauration de l'infrastructure : redéploiement des piles existantes, sur la base de modèles de piles touchées, et lancement d'une restauration des données en fonction du dernier point de restauration connu, sauf indication contraire de votre part, lorsque la résolution de l'incident n'est pas possible.

Termes relatifs à l'infrastructure :

- Environnement de production géré : compte client sur lequel résident les applications de production du client.
- Environnement géré hors production : compte client contenant uniquement des applications hors production, telles que des applications de développement et de test.
- Pile AMS : groupe d'une ou plusieurs AWS ressources gérées par AMS comme une seule unité.
- Infrastructure immuable : modèle de maintenance d'infrastructure typique des groupes Amazon EC2 Auto Scaling (ASGs) dans lequel les composants d'infrastructure mis à jour (dans AWS l'AMI) sont remplacés à chaque déploiement, au lieu d'être mis à jour sur place. L'avantage d'une infrastructure immuable est que tous les composants restent dans un état synchrone puisqu'ils sont toujours générés à partir de la même base. L'immuabilité est indépendante de tout outil ou flux de travail utilisé pour créer l'AMI.
- Infrastructure mutable : modèle de maintenance d'infrastructure typique pour les stacks qui ne sont pas des groupes Amazon EC2 Auto Scaling et qui contiennent une seule instance ou seulement quelques instances. Ce modèle représente le plus fidèlement le déploiement de système traditionnel basé sur le matériel, dans lequel un système est déployé au début de son cycle de vie, puis des mises à jour sont ajoutées à ce système au fil du temps. Toute mise à jour du système est appliquée aux instances individuellement et peut entraîner une interruption du système (selon la configuration de la pile) en raison du redémarrage de l'application ou du système.
- Groupes de sécurité : pare-feux virtuels permettant à votre instance de contrôler le trafic entrant et sortant. Les groupes de sécurité agissent au niveau instance, et non au niveau sous-réseau. Par conséquent, un ensemble différent de groupes de sécurité peut être attribué à chaque instance d'un sous-réseau de votre VPC.
- Contrats de niveau de service (SLAs) : partie des contrats que vous concluez avec AMS et qui définissent le niveau de service attendu.
- SLA non disponible et indisponibilité :
  - Une demande d'API que vous avez soumise qui entraîne une erreur.
  - Une demande de console que vous avez soumise qui entraîne une réponse HTTP 5xx (le serveur est incapable d'exécuter la demande).
  - Toutes les Service AWS offres constituant des piles ou des ressources au sein de votre infrastructure gérée par AMS sont en état de « rupture de service », comme indiqué dans le Service Health Dashboard.
  - L'indisponibilité résultant directement ou indirectement d'une exclusion d'AMS n'est pas prise en compte pour déterminer l'éligibilité aux crédits de service. Les services sont considérés comme disponibles sauf s'ils répondent aux critères d'indisponibilité.

- Objectifs de niveau de service (SLOs) : partie des contrats que vous avez conclus avec AMS qui définissent des objectifs de service spécifiques pour les services AMS.

Conditions d'application des correctifs :

- Correctifs obligatoires : mises à jour de sécurité critiques pour résoudre les problèmes susceptibles de compromettre l'état de sécurité de votre environnement ou de votre compte. Une « mise à jour de sécurité critique » est une mise à jour de sécurité considérée comme « critique » par le fournisseur d'un système d'exploitation compatible avec AMS.
- Correctifs annoncés ou publiés : les correctifs sont généralement annoncés et publiés selon un calendrier. Les correctifs émergents sont annoncés lorsque le besoin du correctif a été découvert et, généralement, peu de temps après, le correctif est publié.
- Module complémentaire de correctif : application de correctifs basée sur des balises pour les instances AMS qui exploite les fonctionnalités AWS Systems Manager (SSM) afin que vous puissiez étiqueter des instances et leur faire appliquer des correctifs à l'aide d'une ligne de base et d'une fenêtre que vous configurez.
- Méthodes de correction :
  - Application de correctifs sur place : application de correctifs effectuée en modifiant des instances existantes.
  - Correctif de remplacement de l'AMI : application de correctifs effectuée en modifiant le paramètre de référence de l'AMI d'une configuration de lancement de groupe EC2 Auto Scaling existante.
- Fournisseur de correctifs (fournisseurs de systèmes d'exploitation, tiers) : les correctifs sont fournis par le fournisseur ou l'organe directeur de l'application.
- Types de correctifs :
  - Mise à jour de sécurité critique (CSU) : mise à jour de sécurité considérée comme « critique » par le fournisseur du système d'exploitation pris en charge.
  - Mise à jour importante (IU) : mise à jour de sécurité considérée comme « importante » ou mise à jour non liée à la sécurité considérée comme « critique » par le fournisseur du système d'exploitation pris en charge.
  - Autre mise à jour (OU) : mise à jour par le fournisseur d'un système d'exploitation pris en charge qui n'est ni un CSU ni une interface utilisateur.
- Correctifs pris en charge : AMS prend en charge les correctifs au niveau du système d'exploitation. Les mises à niveau sont publiées par le fournisseur pour corriger des failles de sécurité ou d'autres

bogues ou pour améliorer les performances. Pour obtenir la liste des configurations actuellement prises en charge OSs, consultez la section Configurations de support.

Termes de sécurité :

- Detective Controls : bibliothèque de moniteurs créés ou activés par AMS qui fournissent une surveillance continue des environnements gérés par les clients et des charges de travail pour les configurations qui ne sont pas conformes aux contrôles de sécurité, opérationnels ou clients, et qui prennent des mesures en informant les propriétaires, en modifiant ou en mettant fin aux ressources de manière proactive.

Modalités de la demande de service :

- Demande de service : demande de votre part concernant une action que vous souhaitez qu'AMS entreprenne en votre nom.
- Notification d'alerte : notification publiée par AMS sur votre page de liste de demandes de service lorsqu'une alerte AMS est déclenchée. Le contact configuré pour votre compte est également averti par la méthode configurée (par exemple, e-mail). Si vous avez des balises de contact sur vos instances/ressources et que vous avez donné votre accord à votre responsable de prestation de services cloud (CSDM) pour les notifications basées sur des balises, les informations de contact (valeur clé) figurant dans la balise sont également notifiées pour les alertes AMS automatisées.
- Notification de service : notification d'AMS publiée sur votre page de liste de demandes de service.

Termes divers :

- Interface AWS Managed Services : pour AMS : la console AWS Managed Services Advanced, l'API AMS CM et Support l'API. Pour AMS Accelerate : la Support console et Support l'API.
- Satisfaction client (CSAT) : AMS CSAT s'appuie sur des analyses approfondies, notamment des évaluations de correspondance pour chaque cas ou correspondance lorsqu'elle est envoyée, des enquêtes trimestrielles, etc.
- DevOps: DevOps est une méthodologie de développement qui préconise fortement l'automatisation et le suivi à toutes les étapes. DevOps vise à raccourcir les cycles de développement, à augmenter la fréquence des déploiements et à rendre les versions plus fiables en réunissant les fonctions traditionnellement distinctes du développement et des opérations sur une base d'automatisation. Lorsque les développeurs peuvent gérer les opérations et que les

opérations informent le développement, les problèmes sont découverts et résolus plus rapidement, et les objectifs commerciaux sont plus facilement atteints.

- ITIL : Information Technology Infrastructure Library (appelée ITIL) est un framework ITSM conçu pour standardiser le cycle de vie des services informatiques. L'ITIL est organisé en cinq étapes qui couvrent le cycle de vie des services informatiques : stratégie des services, conception des services, transition des services, fonctionnement des services et amélioration des services.
- Gestion des services informatiques (ITSM) : ensemble de pratiques qui alignent les services informatiques sur les besoins de votre entreprise.
- Services de surveillance gérés (MMS) : AMS exploite son propre système de surveillance, le Managed Monitoring Service (MMS), qui prend en compte les événements de AWS santé et agrège les données d' CloudWatch Amazon, ainsi que les données provenant Services AWS d'autres fournisseurs, en informant les opérateurs AMS (en ligne 24 heures sur 24, 7 jours sur 7) de toute alarme créée par le biais d'une rubrique Amazon Simple Notification Service (Amazon SNS).
- Espace de noms : lorsque vous créez des politiques IAM ou que vous travaillez avec Amazon Resource Names (ARNs), vous les identifiez Service AWS en utilisant un espace de noms. Vous utilisez les espaces de noms lors de l'identification des actions et des ressources.

Service description (Description du service)

AMS Accelerate est un plan d'exploitation du service AWS Managed Services destiné à gérer les opérations de votre AWS infrastructure.

Fonctionnalités du plan d'exploitation AWS Managed Services (AMS) AMS Accelerate

AMS Accelerate propose les fonctionnalités suivantes :

- Gestion des incidents :

  La gestion des incidents est le processus utilisé par le service AMS pour répondre aux incidents que vous avez signalés.

  AMS Accelerate détecte les incidents et y répond de manière proactive et aide votre équipe à résoudre les problèmes. Vous pouvez contacter les ingénieurs des opérations d'AMS Accelerate 24 heures sur 24, 7 jours sur 7 via le AWS Support Center, le temps de réponse SLAs dépendant du niveau de réponse que vous avez sélectionné pour votre compte.

- Surveillance :

  La surveillance est le processus utilisé par le service AMS pour suivre vos ressources.

  Les comptes inscrits à AMS Accelerate sont configurés avec un déploiement de base d' CloudWatch événements et d'alarmes Amazon qui a été optimisé pour réduire le bruit et identifier un éventuel incident à venir. Après avoir reçu les alertes, l'équipe AMS utilise des mesures correctives, des personnes et des processus automatisés pour remettre les ressources en bon état et communiquer avec vos équipes le cas échéant afin de fournir des informations sur les enseignements à tirer sur le comportement et les moyens de le prévenir. En cas d'échec de la correction, AMS lance le processus de gestion des incidents. Vous pouvez modifier les lignes de base en mettant à jour le fichier de configuration par défaut.

- Sécurité:

  La gestion de la sécurité est le processus utilisé par le service AMS pour protéger vos ressources. AWS Managed Services protège vos actifs informationnels et contribue à la sécurité de votre infrastructure AWS en utilisant plusieurs contrôles, notamment AWS Config Rules et Amazon GuardDuty.

  AMS Accelerate gère une bibliothèque AWS Config Rules de mesures correctives pour garantir que tous vos comptes sont conformes aux normes du secteur en matière de sécurité et d'intégrité opérationnelle. AWS Config Rules suit en permanence le changement de configuration parmi vos ressources enregistrées. Si une modification enfreint l'une des conditions des règles, AMS communique ses conclusions et vous permet de remédier aux violations automatiquement ou sur demande, en fonction de la gravité de la violation. AWS Config Rules faciliter le respect des normes établies par : le Center for Internet Security (CIS), le cadre de sécurité cloud (CSF) du National Institute of Standards and Technology (NIST), le Health Insurance Portability and Accountability Act (HIPAA) et le standard de sécurité des données (DSS) du secteur des cartes de paiement (PCI).

  En outre, AMS Accelerate utilise Amazon GuardDuty pour identifier les activités potentiellement non autorisées ou malveillantes dans votre environnement AWS. GuardDuty les résultats sont surveillés 24 heures sur 24, 7 jours sur 7 par AMS. AMS collabore avec vous pour comprendre l'impact des résultats et des mesures correctives sur la base des recommandations relatives aux meilleures pratiques. AMS aide également Amazon Macie à protéger vos données sensibles telles que les informations médicales personnelles (PHI), les informations personnelles identifiables (PII) et les données financières. Enfin, AMS surveille et trie tous les événements Amazon Route

53 Resolver ALERT et BLOCK générés dans les comptes gérés afin de mieux inspecter le trafic réseau et d'augmenter ses capacités de détection.

- Gestion des correctifs :

  La gestion des correctifs est le processus utilisé par le service AMS pour mettre à jour vos ressources.

  Pour un AWS compte doté du module complémentaire correctif, AWS Managed Services applique et installe les mises à jour des fournisseurs sur les EC2 instances Amazon pour les systèmes d'exploitation pris en charge pendant les périodes de maintenance que vous avez choisies. AMS crée un instantané de l'instance avant d'appliquer le correctif, surveille l'installation du correctif et vous informe du résultat. Si le correctif échoue, AMS enquête sur la panne et vous recommande un plan d'action pour remédier au problème. Ou bien, AMS restaure l'instance pour qu'elle soit annulée, si cela est demandé. AMS fournit des rapports sur la couverture de conformité des correctifs et vous conseille sur la marche à suivre recommandée pour votre entreprise.

- Gestion des sauvegardes :

  AMS utilise la gestion des sauvegardes pour prendre des instantanés de vos ressources.

  AWS Managed Services crée, surveille et stocke des instantanés pour les AWS services pris en charge par AWS Backup. Vous définissez les calendriers, la fréquence et la période de rétention des sauvegardes en créant des AWS Backup plans lors de l'intégration des comptes et des applications. Vous associez les plans aux ressources. AMS suit toutes les tâches de sauvegarde et, en cas d'échec d'une tâche de sauvegarde, alerte notre équipe pour qu'elle procède à une correction. AMS utilise vos instantanés pour effectuer des actions de restauration lors d'incidents, si nécessaire. AMS vous fournit un rapport de couverture de sauvegarde et un rapport d'état des sauvegardes.

- Gestion des problèmes :

  AMS effectue une analyse des tendances afin d'identifier et d'étudier les problèmes et d'en identifier la cause première. Les problèmes sont résolus soit par une solution de contournement, soit par une solution permanente qui empêche qu'un impact similaire sur le service ne se reproduise à l'avenir. Un rapport post-incident (PIR) peut être demandé pour tout incident « élevé », une fois résolu. Le PIR capture la cause première et les mesures préventives prises, y compris la mise en œuvre de mesures préventives.

- Experts désignés :

AMS Accelerate désigne également un responsable de la prestation de services cloud (CSDM) et un architecte cloud (CA) pour établir un partenariat avec votre organisation et promouvoir l'excellence opérationnelle et en matière de sécurité. Votre CSDM et votre CA vous fournissent des conseils pendant et après la configuration et l'intégration d'AMS Accelerate, fournissent un rapport mensuel sur vos indicateurs opérationnels et travaillent avec vous pour identifier les économies potentielles à l'aide d'outils tels qu'AWS Cost Explorer, les rapports sur les coûts et l'utilisation, et. Trusted Advisor

- Outils d'exploitation :

  AMS Accelerate peut fournir des opérations continues pour l'infrastructure de votre charge de travail dans AWS. Nos services de correctifs, de sauvegarde, de surveillance et de gestion des incidents dépendent de l'étiquetage des ressources, ainsi que de l'installation et de la configuration du AWS Systems Manager (SSM) et des CloudWatch agents sur vos EC2 instances Amazon avec un profil d'instance IAM qui les autorise à interagir avec les services SSM et Amazon. CloudWatch AMS Accelerate fournit des outils tels que Resource Tagger pour vous aider à étiqueter vos ressources en fonction de règles, et une configuration d'instance automatisée pour installer les agents requis dans vos EC2 instances Amazon. Si vous suivez des pratiques d'infrastructure immuables, vous pouvez remplir les conditions requises directement dans la console ou infrastructure-as-code dans les modèles.

- Optimisation des coûts :

  AMS Resource Scheduler automatise le démarrage et l'arrêt des instances Amazon Elastic Compute Cloud (Amazon EC2), des instances Amazon Relational Database Service (Amazon RDS) et des groupes Amazon Auto Scaling. EC2 AMS Resource Scheduler vous aide à réduire les coûts opérationnels en arrêtant les ressources qui ne sont pas utilisées et en les redémarrant lorsque leur capacité est nécessaire.

- Journalisation et création de rapports :

  AWS Managed Services agrège et stocke les journaux générés à la suite d'opérations dans et dans CloudWatch Amazon VPC Flow Logs. CloudTrail La journalisation depuis AMS permet d'accélérer la résolution des incidents et les audits du système. AMS Accelerate vous fournit également un rapport de service mensuel qui résume les principaux indicateurs de performance d'AMS, notamment un résumé et des informations, des indicateurs opérationnels, des ressources gérées, le respect des accords de niveau de service (SLA) AMS et des indicateurs financiers relatifs aux dépenses, aux économies et à l'optimisation des coûts. Les rapports sont fournis par le responsable de prestation de services cloud (CSDM) d'AMS qui vous a été désigné.

- Gestion des demandes de service :

  Pour demander des informations sur votre environnement géré, AMS ou vos offres de AWS services, soumettez des demandes de service à l'aide de la console AMS Accelerate. Vous pouvez soumettre une demande de service pour des questions « Comment faire » sur les AWS services et les fonctionnalités ou pour demander des services AMS supplémentaires.

Tous les clients d'AMS Accelerate commencent par la gestion des incidents, la surveillance, la surveillance de la sécurité, l'enregistrement des journaux, les outils prérequis, la gestion des sauvegardes et les fonctionnalités de reporting. Vous pouvez ajouter le module complémentaire de gestion des patchs AMS moyennant un supplément.

> **Note**
>
> Pour obtenir la liste des fonctionnalités non prises en charge dans AWS GovCloud (US), voir En quoi AMS Accelerate diffère pour AWS GovCloud (US)

Configurations prises en charge

AMS Accelerate prend en charge les configurations suivantes :

- Langue : anglais
- Régions : consultez les AWS régions prises en charge par AWS Managed Services sur la page Web des services AWS régionaux.

  > **Note**
  >
  > Les régions AWS introduites avant le 20 mars 2019 sont considérées comme des régions « d'origine » et sont activées par défaut. Les régions introduites après cette date sont des régions « optionnelles » et sont désactivées par défaut. Si votre compte utilise plusieurs régions et que vous intégrez AMS Accelerate à un compte dont la région « opt-in » est activée comme région par défaut, la fonctionnalité de reporting AMS n'est disponible que dans cette région. Si vous ne définissez pas de région par défaut, la dernière région que vous avez visitée est votre région par défaut.
  > Pour activer une région, reportez-vous à la section Activation d'une région. Pour définir une région par défaut, voir Choisir une région. Pour obtenir la liste du statut d'opt-in pour

chaque région, consultez la section Régions disponibles dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud.

- Architecture du système d'exploitation (x86-64 ou ARM64) : toute architecture prise en charge par Systems Manager et. CloudWatch
- Systèmes d'exploitation pris en charge :
  - AlmaLinux 8.3-8.9, 9.x (uniquement AlmaLinux compatible avec l'architecture x86)
  - Amazon Linux 2023
  - Amazon Linux 2 (date de fin de support AMS prévue le 30 juin 2026)
  - Oracle Linux 9.x, 8.x
  - Red Hat Enterprise Linux (RHEL) 9.x, 8.x
  - Serveur SUSE Linux Enterprise 15 SP6
  - SUSE Linux Enterprise Server pour SAP 15 SP3 et versions ultérieures
  - Microsoft Windows Server 2022, 2019, 2016
  - Ubuntu 20.04, 22.04, 24.04
- Systèmes d'exploitation EOS (End of Support) pris en charge :

> **Note**
>
> Les systèmes d'exploitation en fin de support (EOS) sont en dehors de la période de support général du fabricant du système d'exploitation et présentent des risques de sécurité accrus. Les systèmes d'exploitation EOS sont considérés comme des configurations prises en charge uniquement si les agents requis par AMS prennent en charge le système d'exploitation et...
>
> 1. vous bénéficiez d'un support étendu auprès du fournisseur du système d'exploitation qui vous permet de recevoir des mises à jour, ou
> 2. toutes les instances utilisant un système d'exploitation EOS suivent les contrôles de sécurité spécifiés par AMS dans le guide de l'utilisateur Accelerate, ou
> 3. vous vous conformez à tout autre contrôle de sécurité compensatoire exigé par AMS.
>
> Si AMS n'est plus en mesure de prendre en charge un système d'exploitation EOS, AMS émet une recommandation critique pour mettre à niveau le système d'exploitation.

Les agents requis par AMS peuvent inclure, sans toutefois s'y limiter : AWS Systems Manager Amazon CloudWatch, l'agent Endpoint Security (EPS) et le pont Active Directory (AD) (Linux uniquement).

- Ubuntu Linux 18.04
- SUSE Linux Enterprise Server 15 SP3 SP4, et SP5
- Serveur SUSE Linux Enterprise pour SAP 15 SP2
- Serveur SUSE Linux Enterprise 12 SP5
- SUSE Linux Enterprise Service pour SAP 12 SP5
- Microsoft Windows Server 2012/2012 R2
- Red Hat Enterprise Linux (RHEL) :7.x
- Oracle Linux 7.5-7.9

- Si vous avez l' AWS Control Tower habitude de gérer votre environnement multi-comptes, assurez-vous que vous utilisez la dernière version de AWS Control Tower pour garantir la compatibilité avec Accelerate. Les environnements qui utilisent AWS Control Tower des versions antérieures à 2.7 (publiées en avril 2021) ne sont pas pris en charge. Pour plus d'informations sur la procédure de mise à jour AWS Control Tower, voir Mettre à jour votre zone d'atterrissage.

Services pris en charge

AWS Managed Services fournit des services de support à la gestion opérationnelle pour les AWS services suivants. Chaque AWS service étant distinct, le niveau de soutien à la gestion opérationnelle d'AMS varie en fonction de la nature et des caractéristiques du AWS service sous-jacent. Si vous demandez à AWS Managed Services de fournir des services pour un logiciel ou un service qui n'est pas expressément identifié comme pris en charge dans la liste suivante, tout AWS Managed Services fourni pour ces configurations demandées par le client sera traité comme un « service bêta » conformément aux conditions de service.

- Incidents : tous les AWS services
- Demande de service : Tous les AWS services
- Corriger : Amazon EC2

- Sauvegardes et restauration : toutes Services AWS prises en charge par AWS Backup. Pour obtenir la liste des services pris en charge par AWS Backup, consultez les ressources AWS Backup prises en charge.
- Planificateur de ressources : instances Amazon Elastic Compute Cloud EC2 (Amazon), groupes Amazon Relational Database Service (Amazon RDS) et Amazon Auto Scaling EC2
- Services surveillés en fonction des événements opérationnels : vérifications prises en charge et Application Load Balancer Trusted Advisor, Aurora EC2, Amazon, Elastic Load Balancing, Amazon FSx for NetApp ONTAP, Amazon FSx pour Windows File Server, passerelle NAT (un service de traduction d'adresses réseau (NAT)), Amazon AWS Health Dashboard Redshift OpenSearch, Amazon Relational Database Service (Amazon RDS), VPN. Site-to-Site Pour en savoir plus sur ce qu'AMS Accelerate surveille dans le cadre d'un service, consultez la section Alertes issues de la surveillance de base dans AMS.
- Services surveillés par des règles de configuration de sécurité : AWS Account GuardDuty, Macie, Amazon API Gateway,, AWS Certificate Manager, AWS Config,, CloudTrail, CloudWatch, AWS CodeBuild AWS Database Migration Service, Amazon DynamoDB, Amazon, Amazon, EC2 ElastiCache Amazon Elastic Block Store (Amazon EBS), Amazon Elastic File System (Amazon EFS), Amazon Elastic Kubernetes Service (Amazon EKS), Elastic Load Balancing OpenSearch , Amazon Service, Amazon AWS Key Management Service EMR, (IAM AWS Lambda),,, AWS Identity and Access Management Amazon Redshift, Amazon Relational Database Service, Amazon S3, Amazon AI, SageMaker AWS Secrets Manager Amazon Simple Notification Service AWS Systems Manager, Amazon VPC (groupe de sécurité, volume, adresse IP élastique, connexion VPN, passerelles Internet), Amazon VPC Flow Logs. Pour de plus amples informations, veuillez consulter Conformité des configurations dans Accelerate et Protection des données dans Accelerate. Vous trouverez des informations supplémentaires sur la sécurité AMS dans notre guide de sécurité privé AWS Artifact, accessible via l'onglet Reports pour AWS Managed Services.

> **Note**
>
> AMS Accelerate pour la région du Moyen-Orient (Émirats arabes unis) prend en charge un ensemble de fonctionnalités incluses, comme décrit dans le tableau suivant. L'accès à la console du compte AMS et aux instances de cette région est régi exclusivement par des déclencheurs de demandes de service entrantes. Pour plus d'informations sur la disponibilité d'Accelerate dans la région du Moyen-Orient (Émirats arabes unis), consultez votre responsable de compte ou votre responsable de prestation de services AWS cloud (CSDM).

Fonctionnalités incluses dans le champ d'application d'AMS Accelerate pour la région du Moyen-Orient (EAU)	Description de la fonctionnalité
Gestion des incidents	AMS fournit une réponse aux incidents et une assistance pour aider votre équipe à résoudre les problèmes. Pour qu'AMS puisse vous aider à gérer les incidents, vous devez soumettre une demande de service. AMS ne détecte ni ne répond de manière proactive aux incidents dans cette région.
Surveillance	Après avoir reçu une demande de service de votre part, AMS peut vous aider à corriger les ressources. AMS utilise des mesures correctiv es, des personnes et des processus automatis és pour rétablir la santé de vos ressource s. AMS ne configure pas les CloudWatch événements et les alarmes de base dans cette région. Si vous disposez d'outils de surveillance existants, un suivi proactif de vos ressources peut être disponible sur la base de l'évaluation de Cloud Architect (CA) et du CSDM.
Sécurité	Après avoir reçu une demande de service de votre part, AMS peut vous aider à résoudre les problèmes de sécurité. AMS ne déploie pas de contrôles de sécurité tels que et/ou AWS Config Rules ne surveille pas les résultats de sécurité dans cette région. GuardDuty Si vous disposez d'outils de sécurité existants, une surveillance proactive de la sécurité peut être disponible sur la base de l'évaluation de l'autorit é de certification et du CSDM.
Gestion des correctifs	AMS peut appliquer les mises à jour des fournisseurs aux EC2 instances Amazon pour

Fonctionnalités incluses dans le champ d'application d'AMS Accelerate pour la région du Moyen-Orient (EAU)	Description de la fonctionnalité
	les systèmes d'exploitation pris en charge pendant les périodes de maintenance choisies, et créer des instantanés avant l'application des correctifs. Pour qu'AMS puisse vous aider à gérer les correctifs, vous devez soumettre une demande de service. Les notifications et rapports relatifs aux correctifs AMS ne sont pas disponibles dans cette région.
Gestion des sauvegardes	AMS peut créer et stocker des instantanés destinés à être Services AWS pris en charge par AWS Backup et aider à la correction des sauvegardes. Pour qu'AMS puisse vous aider à gérer les sauvegardes, vous devez soumettre une demande de service. AMS ne suit pas les tâches de sauvegarde dans cette région.
Experts désignés	AMS désigne un architecte cloud (CA) et un responsable de la prestation de services cloud (CSDM) pour établir des partenariats avec les organisations clientes et promouvoir l'excelle nce opérationnelle et en matière de sécurité.
Gestion des demandes de service	Pour demander des informations sur votre environnement géré, AMS ou vos Service AWS offres, soumettez des demandes de service via la console AMS Accelerate. Vous pouvez soumettre une demande de service pour des questions « Comment faire » sur Services AWS les fonctionnalités ou pour demander les services AMS disponibles dans cette région, comme décrit dans ce tableau.

Rôles et responsabilités

La matrice AMS Accelerate responsable, responsable, consultée et informée, ou RACI, attribue la responsabilité principale soit au client, soit à AMS pour diverses activités. Le tableau décrit vos responsabilités (le « client ») par rapport aux nôtres (« AMS Accelerate »).

La Étendue des modifications effectuées par AMS Accelerate section répertorie les circonstances spécifiques dans lesquelles AMS est autorisée à apporter des modifications à votre compte, ainsi que certains types de modifications qu'AMS n'effectue jamais.

Matrice RACI AMS Accelerate

AMS Accelerate gère votre infrastructure AWS. Le tableau suivant fournit une vue d'ensemble des rôles et des responsabilités qui vous sont assignés, ainsi qu'à AMS Accelerate, en ce qui concerne les activités du cycle de vie d'une application exécutée dans l'environnement géré.

- R signifie Partie responsable qui fait le travail pour accomplir la tâche.
- C signifie Consulté, une partie dont les opinions sont sollicitées, généralement en tant qu'experts en la matière, et avec laquelle il existe une communication bilatérale.
- Je représente Informed ; une partie qui est informée de l'avancement de la tâche, souvent uniquement à la fin de la tâche.

> **Note**
>
> Certaines sections contiennent un « R » à la fois pour AMS et pour les clients. En effet, dans le modèle de responsabilité AWS partagée, AMS et les clients assument conjointement la responsabilité de répondre aux problèmes d'infrastructure et d'application.

Activité	Client	AWS Managed Services (AMS)
Motifs AMS		
Créez de nouveaux motifs	I	R

Activité	Client	AWS Managed Services (AMS)
Déployez et personnalisez des modèles	R	C, I
Tester et supprimer des modèles	R	I
Cycle de vie des applications		
Développement d'applications	R	I
Exigences, analyse et conception de l'infrastructure des applications	R	I
Déploiement de l'application	R	I
Déploiement des ressources AWS	R	I
Surveillance des applications	R	I
Tests et optimisation des applications	R	I
Résoudre les problèmes liés aux applications	R	I
Résoudre les problèmes et les résoudre	R	I
Surveillance prise en charge pour l'infrastructure AWS	C	R
Réponse aux incidents liés aux problèmes liés au réseau AWS	C	R
Réponse aux incidents liés aux ressources AWS	C	R
Intégration d'un compte géré		
Accordez l'accès au compte géré AWS à l'équipe et aux outils AMS	R	C
Mettez en œuvre des modifications dans le compte ou l'environnement pour permettre le déploiement d'outils dans le compte. Par exemple, modifications des politiques de contrôle des services (SCPs)	R	C

Activité	Client	AWS Managed Services (AMS)
Installation d'agents SSM dans les instances EC2	R	C
Installez et configurez l'outillage requis pour fournir les services AMS. Par exemple, CloudWatch des agents, des scripts pour l'application de correctifs, des alarmes, des journaux, etc.	I	R
Gérez le cycle de vie des accès et des identités pour les ingénieurs AMS	I	R
Collectez toutes les entrées requises pour configurer les services AMS. Par exemple, la durée, le calendrier et les objectifs des fenêtres de maintenance des correctifs	R	I
Demandez la configuration des services AMS et fournissez toutes les entrées requises	R	I
Configurez les services AMS à la demande du client. Par exemple, les fenêtres de maintenance des correctifs, le baliseur de ressources et le gestionnaire d'alarmes	C	R
Gérez le cycle de vie des utilisateurs et leurs autorisations, pour les services d'annuaire locaux, utilisés pour accéder aux comptes et aux instances AWS	R	I
Recommander l'optimisation des instances réservées	I	R
Intégrer un ou plusieurs comptes à Trusted Remediator	C, I	R
Gestion des correctifs		
Collectez toutes les entrées requises pour configurer les fenêtres de maintenance des correctifs, les lignes de base des correctifs et la cible	R	I
Demandez la configuration des fenêtres et des lignes de base de maintenance des correctifs, et fournissez toutes les entrées requises	R	I

Activité	Client	AWS Managed Services (AMS)
Configurer les fenêtres de maintenance des correctifs, les lignes de base des correctifs et les cibles à la demande du client	C	R
Surveillez les mises à jour applicables du système d'exploitation pris en charge et les logiciels préinstallés avec le système d'exploitation pris en charge pour les instances EC2	I	R
Signalement des mises à jour manquantes des systèmes d'exploitation pris en charge et couverture de la période de maintenance	I	R
Prendre des instantanés des instances avant d'appliquer les mises à jour	I	R
Appliquer les mises à jour aux EC2 instances selon la configuration du client	I	R
Examiner les échecs de mise à jour EC2 des instances	C	R
Mise à jour AMIs et piles pour les groupes Auto-Scaling () ASGs	R	C
Corrigez le système d'exploitation Windows et les packages Microsoft installés sur le système d'exploitation qui sont régis par Windows Update	I	R
Corrigez les applications installées, les logiciels ou les dépendances d'applications non gérés par Windows Update	R	I
Appliquez des correctifs au système d'exploitation Linux et à tout package dont la gestion est activée par le gestionnaire de packages natif du système d'exploitation (par exemple Yum, Apt, Zypper)	I	R
Corrigez les applications installées, les logiciels ou les dépendanc es d'applications non gérés par le gestionnaire de packages natif du système d'exploitation Linux	R	I
Sauvegarde		

Activité	Client	AWS Managed Services (AMS)
Collectez toutes les entrées requises pour configurer les plans de sauvegarde et les ressources cibles	R	I
Demandez la configuration des plans de sauvegarde et fournissez toutes les entrées requises	R	I
Configurer les plans et les cibles de sauvegarde à la demande du client	C	R
Spécifiez les plannings de sauvegarde et les ressources cibles	R	I
Effectuez des sauvegardes selon le plan	I	R
Examiner les tâches de sauvegarde ayant échoué	I	R
Rapport sur l'état des tâches de sauvegarde et la couverture des sauvegardes	I	R
Valider les sauvegardes	R	I
Demandez la restauration des ressources des services AWS pris en charge dans le cadre de la gestion des incidents	R	I
Réaliser des activités de restauration des sauvegardes pour les ressources des services AWS pris en charge	I	R
Restaurez les applications personnalisées ou tierces concernées	R	I
Réseaux		
Approvisionnement et configuration du compte géré VPCs IGWs, de la connexion directe et d'autres services réseau AWS	R	I
Configuration et exploitation d'AWS Security Groups/NAT/NACL dans le compte géré	R	I

Activité	Client	AWS Managed Services (AMS)
Configuration et mise en œuvre du réseau au sein du réseau du client (par exemple DirectConnect)	R	I
Configuration et mise en œuvre du réseau au sein du réseau AWS	R	I
Moniteur défini par AMS pour la sécurité du réseau, y compris les groupes de sécurité	I	R
Configuration et gestion de la journalisation au niveau du réseau (journaux de flux VPC et autres)	I	R
Journalisation		
Enregistrer tous les journaux des modifications apportées aux applicati ons	R	I
Enregistrer les journaux des modifications de l'infrastructure AWS	I	R
Activer et agréger la piste d'audit AWS	I	R
Journaux agrégés issus des ressources AWS	I	R
Surveillance et remédiation		
Collectez toutes les entrées requises pour configurer le gestionnaire d'alarmes, le baliseur de ressources et les seuils d'alarme	R	I
Demandez la configuration du gestionnaire d'alarmes et fournissez toutes les entrées requises	R	I
Configurez le gestionnaire d'alarmes, le baliseur de ressources et les seuils d'alarme à la demande du client.	C	R
Déployez les métriques CloudWatch de base et les alarmes AMS selon la configuration du client	I	R

Activité	Client	AWS Managed Services (AMS)
Surveillez les ressources AWS prises en charge à l'aide de CloudWatch métriques et d'alarmes de base	I	R
Étudier les alertes provenant des ressources AWS	C	R
Corriger les alertes en fonction de la configuration définie ou créer un incident	I	R
Définissez, surveillez et étudiez les moniteurs spécifiques au client	R	I
Étudier les alertes issues de la surveillance des applications	R	C
Configuration Trusted Advisor des contrôles pour la correction	R	C
Corriger automatiquement les vérifications prises en charge Trusted Advisor	I	R
Corriger manuellement les vérifications prises en charge Trusted Advisor	R	C
Signaler l'état de la correction	I	R
Résoudre les problèmes de correction	R	C
Architecture de sécurité		
Consultez les ressources et le code AMS pour détecter les problèmes de sécurité et les menaces potentielles	I	R
Implémenter des contrôles de sécurité dans les ressources et le code AMS pour atténuer les risques de sécurité	I	R
Activez les services AWS pris en charge pour la gestion de la sécurité du compte et de ses ressources AWS	I	R

Activité	Client	AWS Managed Services (AMS)
Gérez les informations d'identification privilégiées pour l'accès au compte et au système d'exploitation pour les ingénieurs AMS	I	R
Gestion des risques de sécurité		
Surveillez les services AWS pris en charge pour la gestion de la sécurité, comme GuardDuty Macie	I	R
Définissez et créez des règles de configuration définies par AMS pour détecter si les ressources AWS sont conformes aux meilleures pratiques de sécurité du Center for Internet Security (CIS) et du NIST.	I	R
Surveiller les règles de configuration définies par AMS	I	R
Signaler l'état de conformité des règles de configuration	I	R
Définissez une liste des règles de configuration requises et corrigez-les	I	R
Évaluez l'impact de la correction des règles de configuration définies par AMS	R	I
Demander la correction des règles de configuration définies par AMS dans le compte AWS	R	I
Suivez les ressources exemptées des règles de configuration définies par AMS	R	I
Corriger les règles de configuration définies par AMS prises en charge dans le compte AWS	C	R
Corriger les règles de configuration définies par AMS non prises en charge dans le compte AWS	R	I
Définissez, surveillez et étudiez les règles de configuration spécifiques au client	R	I

Activité	Client	AWS Managed Services (AMS)
Gestion des incidents		
Notifier les incidents détectés par AMS dans les ressources AWS	I	R
Signaler les incidents dans les AWS ressources	R	I
Notifier les incidents relatifs aux AWS ressources sur la base de la surveillance	I	R
Gérez les problèmes de performance et les pannes des applications	R	I
Catégoriser la priorité des incidents	I	R
Fournir une réponse aux incidents	I	R
Assurez la résolution des incidents ou la restauration de l'infrastructure des ressources avec des sauvegardes disponibles	C	R
Réponse aux incidents de sécurité — Préparation		
Communications		
Fournir et mettre à jour les coordonnées de sécurité du client pour qu'AMS puisse les utiliser lors d'événements de sécurité, de notifications et d'escalades de sécurité	R	I
Stockez et gérez les coordonnées de sécurité du client fournies à utiliser lors d'événements de sécurité et d'escalades de sécurité	C	R
Entrainement		
Fournir au client de la documentation pour soutenir AMS pendant le processus de réponse aux incidents	I	R

Activité	Client	AWS Managed Services (AMS)
Pratiquez le partage des responsabilités lors des processus de réponse aux incidents grâce à des journées de jeu sur la sécurité	R	R
Gestion des ressources		
Configuration de la gestion de la sécurité prise en charge Services AWS pour les alertes, la corrélation des alertes, la réduction du bruit et les règles supplémentaires	I	R
Tenez un inventaire complet des AWS ressources (Amazon EC2, Amazon S3, etc.), y compris des informations détaillées sur la valeur et le caractère critique de chaque actif pour l'entreprise. Ces informati ons seront déterminantes pour déterminer une stratégie de confinement efficace.	R	C
Utilisez des AWS balises pour identifier les ressources et les charges de travail	R	C
Définition et configuration de la conservation et de l'archivage des journaux	I	R
Établissez une base de référence sécurisée en définissant et en appliquant les politiques et les configurations de sécurité de l'organis ation pour les AWS comptes, les services et la gestion des accès	R	I
Réponse aux incidents de sécurité - Détecter		
Journalisation, indicateurs et surveillance		
Configurer la journalisation et la surveillance pour permettre la gestion des événements pour les instances et les comptes	I	R
Moniteur pris en charge Services AWS pour les alertes de sécurité	I	R

Activité	Client	AWS Managed Services (AMS)
Déployer et gérer les outils de sécurité des terminaux	R	I
Surveillez les instances pour détecter les malwares à l'aide de la sécurité des terminaux	R	I
Informer le client des événements détectés par le biais de messages sortants	I	R
Coordonner les communications internes avec les parties prenantes et les mises à jour de la direction pour améliorer le temps de réponse	R	I
Définissez, déployez et gérez les services de détection standard AMS (par exemple, Amazon GuardDuty et AWS Config)	C	R
Enregistrer les journaux AWS des modifications de l'infrastructure	R	I
Activer et configurer la journalisation et la surveillance pour permettre la gestion des événements pour l'application	R	C
Implémenter et gérer une liste d'autorisation, une liste de refus et des détections personnalisées sur les services de AWS sécurité pris en charge (par exemple, Amazon) GuardDuty	R	R
Signalement des événements de sécurité		
Signaler à AMS une activité suspecte ou une enquête de sécurité en cours	R	I
Notifier les événements et incidents de sécurité détectés au client	I	R
Notifier un événement planifié susceptible de déclencher le processus de réponse aux incidents de sécurité	R	I
Réponse aux incidents de sécurité - Analyser		

Activité	Client	AWS Managed Services (AMS)
Investigation et analyse		
Réaliser une réponse initiale en cas d'alerte de sécurité prise en charge générée par une source de détection prise en charge	I	R
Évaluez false/true les résultats positifs à l'aide des données disponibles	R	R
Générez un instantané des instances concernées à partager avec le client si nécessaire	I	R
Effectuez des tâches de criminalistique telles que la chaîne de traçabilité, l'analyse du système de fichiers, la criminalistique de la mémoire et l'analyse binaire	R	C
Collectez les journaux des applications pour faciliter les enquêtes	R	I
Collectez des données et des journaux pour faciliter les enquêtes sur les alertes de sécurité	R	R
SMEs Participez Services AWS aux enquêtes de sécurité	C	R
Partagez les journaux d'investigation du support avec Services AWS les clients au cours d'une enquête	I	R
Communication		
Envoyer des alertes et des notifications depuis les sources de détection AMS pour les ressources gérées	I	R
Gérer les alertes et les notifications relatives aux événements liés à la sécurité des applications	R	I
Contacter le point de contact du client chargé de la sécurité lors d'une enquête sur un incident de sécurité	R	I

Activité	Client	AWS Managed Services (AMS)
Réponse aux incidents de sécurité - Contain		
Stratégie de confinement et exécution		
Évaluez les risques et déterminez la stratégie de confinement, en tenant compte des impacts potentiels sur les services	R	C
Effectuez une sauvegarde des systèmes concernés pour une analyse plus approfondie	I	R
Limiter les applications et les charges de travail (par le biais d'une configuration ou d'une activité de réponse spécifique à l'application)	R	C
Définissez la stratégie de confinement en fonction de l'incident de sécurité et de la ressource affectée	I	R
Activez le chiffrement et le stockage sécurisé des sauvegardes ponctuelles des systèmes concernés	C	R
Exécutez les actions de confinement prises en charge pour les AWS ressources, notamment EC2 les instances, le réseau et l'IAM	I	R
Réponse aux incidents de sécurité - Eradiquer		
Stratégie d'éradication et exécution		
Définissez les options d'éradication en fonction de l'incident de sécurité et de la ressource affectée sur les charges de travail des applications du client	C	R
Décider de la stratégie d'éradication convenue, du calendrier d'exécution de l'éradication et des conséquences	R	I
Définissez les étapes d'éradication en fonction de l'incident de sécurité et de la ressource affectée sur les charges de travail gérées par AMS	C	R

Activité	Client	AWS Managed Services (AMS)
Éliminez les menaces et renforcez les AWS ressources, y compris l'éradication EC2 des instances, du réseau et de l'IAM	R	C
Éradiquer les menaces et renforcer les applications et les charges de travail (par le biais d'une configuration ou d'une activité de réponse spécifique à l'application)	R	I
Réponse aux incidents de sécurité - Restaurer		
Préparation et exécution du rétablissement		
Configurer les plans et les cibles de sauvegarde à la demande du client	I	R
Passez en revue les plans de sauvegarde pour restaurer les charges de travail gérées par AMS	R	I
Effectuez des activités de restauration des sauvegardes pour les ressources prises en charge Services AWS	I	R
Sauvegardez l'application client, la configuration de l'application et les paramètres de déploiement, et passez en revue les plans de sauvegarde pour restaurer les applications et les charges de travail des clients après un incident	R	I
Restaurez les applications et les charges de travail des clients (via des étapes de restauration spécifiques à l'application)	R	I
Réponse aux incidents de sécurité — Rapport post-incident		
Signalement après un incident		
Partagez les leçons apprises et les mesures à prendre avec le client après l'incident, selon les besoins	I	R
Gestion des problèmes		

Activité	Client	AWS Managed Services (AMS)
Corréler les incidents pour identifier les problèmes	I	R
Réaliser une analyse des causes profondes (RCA) en cas de problème	I	R
Corriger les problèmes	I	R
Identifier et résoudre les problèmes liés aux applications	R	I
Gestion des services		
Demander des informations à l'aide de demandes de service	R	I
Répondre aux demandes de service	I	R
Fournir des recommandations d'optimisation des coûts	I	R
Préparer et fournir un rapport de service mensuel	I	R
Gestion du changement		
Processus et outils de gestion du changement pour le provisionnement et la mise à jour des ressources dans l'environnement géré	R	I
Maintenance du calendrier de modification des applications	R	I
Avis concernant la prochaine fenêtre de maintenance	R	I
Enregistrer les modifications apportées par AMS Operations	I	R
Optimisation des coûts		
Collectez toutes les entrées requises pour configurer le planificateur de ressources	R	I
Demandez l'intégration, la configuration du planificateur de ressources et fournissez toutes les informations requises	R	I

Activité	Client	AWS Managed Services (AMS)
Déployer le planificateur de ressources selon la configuration du client	C, I	R
Désactiver et activer le planificateur de ressources sur le compte client	R	C
Création, suppression, description et mise à jour des plannings	C	R
Création, suppression, description et mise à jour de périodes	C	R
Étudier et résoudre les problèmes liés au planificateur de ressources	I	R
Demande de déconnexion du planificateur de ressources	R	I
Déconnecter le planificateur de ressources du compte	C, I	R

Étendue des modifications effectuées par AMS Accelerate

AMS Accelerate apporte des modifications uniquement aux fins et dans les situations spécifiques décrites ci-dessous. AMS apporte des modifications uniquement au niveau de l'infrastructure, à l'aide de la console ou APIs. AMS ne modifie jamais vos couches d'application, de contrôle ou de domaine. Vous pouvez voir toutes les modifications apportées par AMS (ou par d'autres utilisateurs) à l'aide de notre ensemble de requêtes prédéfinies ; pour ce faire, consultezSuivi des modifications apportées à vos comptes AMS Accelerate.

AWS resources

AMS Accelerate déploie ou met à jour AWS les ressources uniquement dans les situations suivantes :

- Déployer et mettre à jour les outils et les ressources requis par AMS.
- Dans le cadre de la surveillance AMS, en réponse à des événements et à des alarmes.
- Corriger les problèmes de sécurité dans le cadre de Réponses aux violations dans Accelerate (mise en conformité des ressources non conformes aux meilleures pratiques de sécurité).
- Pendant la remédiation et la restauration dans le cadre de la réponse à un incident.

- Lorsque vous répondez aux demandes des clients concernant la configuration des fonctionnalités AMS, telles que les suivantes :
  - Gestionnaire d'alarmes
  - Étiqueteur de ressources
  - Lignes de base des correctifs et fenêtres de maintenance
  - Planificateur de ressources
  - Plans de sauvegarde

AMS Accelerate ne déploie ni ne met à jour les ressources en dehors de ces situations. Si vous avez besoin de l'aide d'AMS pour apporter des modifications dans d'autres situations, pensez à utiliser Operations on Demand.

Logiciel du système d'exploitation

AMS Accelerate peut apporter des modifications au logiciel de votre système d'exploitation en cas d'indisponibilité via la résolution des incidents, conformément à notre accord de niveau de service. AMS peut également apporter des modifications à vos systèmes d'exploitation dans le cadre deConfiguration d'instance automatisée dans AMS Accelerate.

Code et configuration de l'application

AMS Accelerate ne modifie jamais votre code (par exemple, les CloudFormation modèles AWS, d'autres infrastructure-as-code modèles ou les fonctions Lambda), mais peut indiquer à vos équipes quelles modifications sont nécessaires pour suivre les meilleures pratiques opérationnelles et de sécurité. AMS Accelerate fournit une assistance pour résoudre les problèmes d'infrastructure qui ont un impact sur les applications, mais AMS Accelerate n'accède pas aux configurations de vos applications et ne les valide pas.

Fonctionnalités pour les systèmes d'exploitation non pris en charge dans Accelerate

Un système d'exploitation non pris en charge est un système d'exploitation non répertorié dans leConfigurations prises en charge. AMS considère les instances dont les systèmes d'exploitation ne sont pas pris en charge comme des « configurations demandées par le client » soumises aux conditions de service des versions AWS bêta et préliminaire.

L'ensemble limité de fonctionnalités AMS suivant est disponible pour les instances dont les systèmes d'exploitation ne sont pas pris en charge :

Capacité	Remarques
Gestion des incidents	AMS fournit une réponse aux incidents.
Gestion des demandes de service	AMS répond aux demandes de service.
Surveillance	AMS surveille et répond aux vérifications de l'état EC2 du système Amazon et aux vérifications de l'état des instances. Les vérifications de l'état du système incluent : la perte de connectivité réseau, la perte d'alimentation du système, les problèmes logiciels sur l'hôte physique et les problèmes matériels sur l'hôte physique qui ont une incidence sur l'accessibilité du réseau. Les vérifications de l'état des instances incluent : une configuration réseau ou de démarrage incorrecte, une mémoire épuisée, un système de fichiers endommagé et un noyau incompatible.
Gestion de la sécurité	AMS surveille les EC2 GuardDuty conclusions et les AWS Config règles d'Amazon et y répond.
Gestion des sauvegardes	AMS assure la gestion de la continuité dans Accelerate pour EC2 l'utilisation de AWS Backup plans et de coffres-forts personnalisés par AMS.

Contact et escalade

Vous avez un responsable de prestation de services cloud (CSDM) désigné qui fournit une assistance consultative sur AMS Accelerate et possède une compréhension détaillée de votre cas d'utilisation et de votre architecture technologique pour l'environnement géré. CSDMs travailler avec les responsables de comptes, les responsables de comptes techniques, les architectes cloud AWS Managed Services (CAs) et les architectes de solutions AWS (SAs), le cas échéant, pour aider à lancer de nouveaux projets et fournir des recommandations de bonnes pratiques tout au long des

processus de développement et d'exploitation des logiciels. Le CSDM est le principal point de contact pour AMS. Les principales responsabilités de votre CSDM sont les suivantes :

- Organisez et animez des réunions mensuelles d'évaluation des services avec les clients.
- Fournissez des détails sur la sécurité, les mises à jour logicielles pour l'environnement et les opportunités d'optimisation.
- Répondez à vos exigences, y compris les demandes de fonctionnalités pour AMS Accelerate.
- Répondez aux demandes de facturation et de rapports de service et résolvez-les.
- Fournissez des informations pour les recommandations d'optimisation financière et de capacité.

Heures de contact

Vous pouvez contacter AMS Accelerate pour différentes raisons et à différents moments.

Fonctionnalité	AMS Accelerate
	Niveau Premium
Demande de service	24 h/24,
Gestion des incidents (P2-P3)	24 h/24,
Sauvegarde et restauration	24 h/24,
Gestion des correctifs	24 h/24,
Surveillance et alertes	24 h/24,
Responsable de la prestation de services cloud (CSDM)	Du lundi au vendredi : de 8h00 à 17h00, heures d'ouverture locales

Heures d'ouverture

Fonctionnalité	AMS Accelerate
	Niveau Premium
Demande de service	24/7
Gestion des incidents (P1)	24/7
Gestion des incidents (P2-P3)	24/7
Sauvegarde et restauration	24/7
Gestion des correctifs	24/7
Surveillance et alertes	24/7
Responsable de la prestation de services cloud (CSDM)	Du lundi au vendredi : de 9h00 à 17h00, heures d'ouverture locales

Voie d'escalade

AMS soutient ses clients en matière de gestion des incidents et de gestion des demandes de service, 24 heures sur 24, 7 jours sur 7, 365 jours par an, conformément au contrat de niveau de service AMS appliqué au compte.

Pour signaler un problème de performance des services AWS ou AMS ayant une incidence sur votre environnement géré, utilisez la console AMS et soumettez un dossier d'incident. Pour en savoir plus, consultez Soumission d'un incident pour Accelerate. Pour des informations générales sur la gestion des incidents AMS, consultezGestion des incidents dans AMS Accelerate.

Pour demander des informations ou des conseils, ou pour demander des services supplémentaires à AMS, utilisez la console AMS et soumettez une demande de service. Pour en savoir plus, consultez Création d'une demande de service dans Accelerate. Pour des informations générales sur les demandes de service AMS, consultezGestion des demandes de service dans Accelerate.

Inventaire des ressources pour Accelerate

Toutes les ressources déployées par AMS Accelerate sur vos comptes Compte AWS OR sont répertoriées dans la feuille de calcul `resource_inventory.zip`resource_inventory.xlsx (compressée).

> **Note**
>
> Dans la colonne Nom de la ressource, le préfixe CFN : indique un identifiant CloudFormation logique au lieu d'un nom de ressource. Elles sont affichées pour les ressources anonymes, par exemple pour les politiques de compartiment S3.

AMS déploie un ensemble de services tels que décrits dans leService description (Description du service). Le coût de leur déploiement est faible lorsqu'ils sont déployés sur un compte vide, mais il augmente à mesure que le taux d'utilisation augmente. Par exemple, des journaux sont créés et des règles de configuration sont invoquées à mesure que les ressources changent.

Lorsque plusieurs modifications sont apportées aux règles de configuration, plusieurs invocations de conformité de configuration peuvent être déclenchées, ce qui entraîne une augmentation des coûts. La même possibilité s'applique à Amazon CloudWatch utilisé pour les instances de surveillance : plus votre surveillance est précise, plus le coût du service est élevé. AWS Backup est un autre exemple. Si vous avez plusieurs sauvegardes stockées ou si vous avez des périodes de rétention plus longues, vous utilisez davantage d'espace de stockage et le coût est plus élevé.

Ces chiffres sont difficiles à prévoir. Lors de votre examen mensuel de votre activité avec votre responsable de la prestation de services cloud (CSDM), suivez les changements et efforcez-vous d'identifier les domaines dans lesquels il est possible de réduire les coûts.

Commencer à utiliser AMS Accelerate

Si vous ne possédez pas encore de compte AWS Managed Services (AMS), commencez par contacter un représentant commercial Amazon Web Services (AWS) via notre page AWS Managed Services - Contact Sales.

Une fois que vous vous êtes inscrit à un AMS, l'équipe AMS Accelerate vous guide tout au long du processus d'intégration suivant pour chacun de vos Comptes AWS.

Consultez l'ensemble des fonctionnalités ici : Fonctionnalités d'AWS Managed Services

> **Note**
>
> AMS Accelerate prend en charge GovCloud les régions. Si votre service doit résider dans un AWS GovCloud (US) Region, voir également Getting Started with AWS GovCloud (US).

Processus d'ouverture de compte pour Accelerate

L'intégration d'un compte dans AMS Accelerate se déroule en quatre étapes.

1. Étape 1. Découverte de comptes dans Accelerateévalue l'état actuel de votre compte et identifie les obstacles techniques à l'intégration de votre compte.
2. Étape 2. Ressources de gestion de l'intégration dans Acceleratevous demande d'accepter les conditions générales et de créer un rôle d'intégration pour les architectes cloud AMS Accelerate (CAs), qui vous aideront à définir une base de sécurité et à résoudre les problèmes si nécessaire.
3. Étape 3. Intégration des fonctionnalités AMS avec des politiques par défautpour les fonctionnalités d'Accelerate, telles que la surveillance, l'application de correctifs et la sauvegarde.
4. Étape 4 : Personnalisez les fonctionnalités dans Acceleratgarantit que les ressources, y compris EC2 les instances, sont correctement configurées pour votre application.

Accélérez les prérequis d'intégration

Avant de commencer le processus d'intégration, il est important de comprendre les dépendances techniques sur lesquelles reposent les composants d'Accelerate.

> **Note**
>
> Pour utiliser AMS Accelerate, vous devez souscrire à l'un des deux Support plans pris en charge : Enterprise On-Ramp ou Enterprise. Les plans Developer et Business ne sont pas éligibles pour bénéficier d'AMS Accelerate. Pour en savoir plus sur les différents forfaits, voir Comparer les Support forfaits.

Points de terminaison VPC AMS Accelerate

Un point de terminaison VPC permet des connexions privées entre votre VPC et les services pris en charge et les services AWS de point de terminaison VPC alimentés par. AWS Si vous devez filtrer la connectivité Internet sortante, configurez les points de terminaison du service VPC suivants pour vous assurer qu'AMS Accelerate est connecté à ses dépendances de service.

> **Note**
>
> Dans la liste suivante, *`region`* représente l'identifiant d'une AWS région, par exemple `us-east-2` pour la région USA Est (Ohio).

```
com.amazonaws.region.logs
com.amazonaws.region.monitoring
com.amazonaws.region.ec2
com.amazonaws.region.ec2messages
com.amazonaws.region.ssm
com.amazonaws.region.ssmmessages
com.amazonaws.region.s3
com.amazonaws.region.events
```

Pour plus d'informations sur la configuration des points de terminaison VPC AWS, consultez la section Points de terminaison VPC.

> **Note**
>
> Si vous créez des points de terminaison VPC dans votre compte pour tous les services mentionnés ci-dessus, consultez cet exemple de modèle. AWS CloudFormation Vous pouvez

mettre à jour ce modèle et supprimer ou ajouter une définition de points de terminaison VPC selon votre cas d'utilisation.

Connectivité Internet sortante dans Accelerate

1. Téléchargement egressMgmt.zip.
2. Ouvrez le fichier **`ams-egress.json`**.
3. URLs Retrouvez-les sous les propriétés JSON :
   - `WindowsPatching`
   - `RedHatPatching`
   - `AmazonLinuxPatching`
   - `EPELRepository`
4. Autorisez l'accès à ces derniers URLs.

Test de la connectivité sortante dans Accelerate

Testez la connectivité sortante à l'aide de l'une des méthodes suivantes.

> **Note**
>
> Avant d'exécuter le script/la commande, remplacez le rouge *`region`* par votre identifiant de région, par exemple. `us-east-1`

PowerShell Script Windows

```
$region = 'region'
@('logs','monitoring','ec2','ec2messages','ssm','ssmmessages','s3','events') | `
ForEach-Object { `
Test-NetConnection ("$_" + '.' + "$region" + '.amazonaws.com') -Port 443 } | `
Format-Table ComputerName,RemotePort,RemoteAddress,PingSucceeded,TcpTestSucceeded -
AutoSize
```

commande Linux

```
for endpoint in logs monitoring ec2 ec2messages ssm ssmmessages s3 events; do nc -zv
 $endpoint.region.amazonaws.com 443; done
```

Amazon EC2 Systems Manager dans Accelerate

Vous devez installer l' AWS Systems Manager agent (agent SSM) sur toutes les EC2 instances que vous souhaitez qu'AMS gère. Vous devez également ajouter les autorisations de compartiment requises par l'agent SSM. Pour un aperçu incluant Amazon EC2, consultezÉtape 3. Intégration des fonctionnalités AMS avec des politiques par défaut.

IAM dans Accelerate

Pour permettre à vos utilisateurs de lire et de configurer les fonctionnalités d'AMS Accelerate, comme l'accès à la console AMS ou la configuration de sauvegardes, vous devez accorder des autorisations explicites dans AWS Identity and Access Management (IAM) pour effectuer ces actions. Par exemple, les politiques IAM, voir Autorisations d'utilisation des fonctionnalités AMS.

Étape 1. Découverte de comptes dans Accelerate

AMS travaille avec vous lors de la découverte du compte afin d'évaluer l'état actuel de votre compte et d'identifier les obstacles techniques à l'intégration de votre compte. AMS ne fournit pas de services opérationnels pendant la phase de découverte du compte. AMS utilise le rôle `AWSServiceRoleForSupport` lié au service pour identifier les bloqueurs techniques, puis travaille avec vous pour y remédier, avant de passer à la phase d'intégration au niveau du compte.

Processus de découverte de comptes dans Accelerate

Pour vous aider à analyser et à découvrir votre compte, AMS effectue des contrôles opérationnels afin d'identifier les bloqueurs techniques par le biais d'appels d'API en lecture seule. Une fois que votre compte est intégré à AMS, ces vérifications sont effectuées à la demande afin de maintenir le profil du compte. AMS travaille avec vous pour corriger les résultats associés à ces contrôles, le cas échéant. AMS utilise les contrôles opérationnels et les actions d'API en lecture seule suivants dans le cadre de Account Discovery :

Contrôle opérationnel	Objectif	AWS Appels d'API utilisés
AWS Control Tower Évaluation des versions	Identifie la AWS Control Tower version pour s'assurer qu'il	• `ControlTower:GetLandingZone`

Contrôle opérationnel	Objectif	AWS Appels d'API utilisés
	s'agit de la version minimale prise en charge pour l'intégration de votre Compte AWS.	• `ControlTower:ListEnabledControls` • `ControlTower:ListLandingZones`
AWS CloudTrail Évaluation	Identifie les AWS CloudTrail sentiers et leurs configurations pour vous intégrer afin de minimiser les coûts liés Compte AWS aux CloudTrail sentiers.	• `CloudTrail:GetTrail` • `CloudTrail:ListTrails` • `S3:GetBucketOwnershipControls` • `S3:GetBucketPolicy` • `KMS:GetKeyPolicy` • `CloudTrail:GetEventSelectors` • `S3:GetBucketLogging` • `S3: GetBucketLifecycleConfiguration` • `S3: GetBucketEncryption`
AWS CloudFormation Évaluation du crochet	Identifie CloudFormation les points de votre intégration Compte AWS qui bloquent le déploiement du service AMS dans votre Compte AWS.	• `CloudFormation:ListTypes`

Contrôle opérationnel	Objectif	AWS Appels d'API utilisés
Évaluation des EC2 instances Amazon	Identifie les EC2 instances de votre Compte AWS ordinateur qui n'exécutent pas AWS Systems Manager l'agent (agent SSM) et qui ne sont pas prises en charge par AMS.	• `EC2:DescribeInstances` • `EC2:DescribeImages` • `SSM:DescribeInstanceInformation`

AMS Accelerate suit les meilleures pratiques du secteur pour respecter et maintenir l'éligibilité en matière de conformité. L'accès à votre compte par AMS Accelerate Discovery est enregistré AWS CloudTrail via le rôle AWSServiceRoleForSupport lié au service. Cela permet de répondre aux exigences de surveillance et d'audit. Pour plus d'informations AWS CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Étape 2. Ressources de gestion de l'intégration dans Accelerate

Voici un aperçu du processus d'intégration des ressources de gestion.

Vous acceptez les conditions

Votre responsable de prestation de services cloud (CSDM) vous guide tout au long du processus d'acceptation. Vous devez accepter les conditions générales, la sélection Régions AWS, les modules complémentaires et un accord de niveau de service (SLA).

Vous accordez des autorisations aux rôles AMS

Vous devez autoriser l'accès aux processus AMS et à votre architecte cloud. Pour ce faire, créez une AWS CloudFormation pile pour chaque rôle. Voir Le modèle pour créer des rôles AMS et ensuiteCréez `aws_managedservices_onboarding_role` avec AWS CloudFormation for Accelerate. Pour de plus amples informations, veuillez consulter Gestion des accès dans AMS Accelerate.

AMS examine votre configuration

Votre architecte cloud (CA) recherche également les éventuels problèmes de configuration de votre compte, tels que les politiques de contrôle des services (SCPs), et les résultats de sécurité susceptibles d'empêcher AMS de déployer les outils et les ressources requis par AMS. Votre autorité

de certification travaille avec vous pour vous aider à corriger les résultats et à supprimer les obstacles au déploiement des outils et ressources AMS.

AMS examine les configurations de vos AWS CloudTrail sentiers

Votre architecte cloud (CA) examinera vos configurations de CloudTrail suivi et confirmera si vous souhaitez qu'AMS déploie un suivi global CloudTrail ou intègre Accelerate aux ressources de suivi de votre CloudTrail compte ou de votre organisation. Si vous choisissez d'intégrer Accelerate à votre CloudTrail sentier, votre autorité de certification vous guidera à travers les mises à jour requises des configurations de vos ressources de CloudTrail sentiers.

AMS déploie des ressources de gestion

L'équipe AMS déploie des outils et des AWS ressources pour fournir les différents services d'AMS Accelerate. Une fois l'opération terminée, AMS a créé le compte AWS Managed Services et AMS vous informe que votre compte est actif.

Ceci conclut la phase des ressources de gestion de l'intégration. Vous pouvez passer directement à l'étape suivante du processus d'intégration :Étape 3. Intégration des fonctionnalités AMS avec des politiques par défaut.

> **Note**
>
> Maintenant que votre compte est actif, vous pouvez effectuer l'une des tâches suivantes :
>
> - Créez des incidents et des demandes de service pour l' AWS infrastructure à l'aide de la console Support Center. Consultez Rapports d'incidents, demandes de service et questions de facturation dans AMS Accelerate.
> - Consultez l'état de conformité des AWS Config règles déployées par AMS dans votre compte. Conformité des configurations dans Accelerate
> - Localisez GuardDuty et analysez les résultats ainsi que Macie (facultatif). Consultez Moniteur avec GuardDuty.
> - CloudTrail Journaux d'accès et d'audit
> - Suivez les modifications apportées à votre compte AMS Accelerate. Consultez Suivi des modifications apportées à vos comptes AMS Accelerate.
> - Utilisez Resource Tagger pour créer des balises. Consultez Accélérez Resource Tagger.
> - Demandez un correctif, une sauvegarde et AWS Config des rapports. Consultez Rapports et options.

Passez en revue et mettez à jour vos configurations pour permettre à AMS Accelerate d'utiliser votre CloudTrail parcours

AMS Accelerate s'appuie sur la AWS CloudTrail connexion pour gérer les audits et la conformité de toutes les ressources de votre compte. Lors de l'intégration, vous choisissez si Accelerate déploie un suivi dans CloudTrail votre AWS région principale ou utilise les événements générés par votre CloudTrail compte existant ou le journal de votre organisation. Si aucun suivi n'est configuré sur votre compte, Accelerate déploiera un suivi géré lors CloudTrail de l'intégration.

> **Important**
>
> CloudTrail la configuration de la gestion des journaux n'est requise que lorsque vous choisissez d'intégrer AMS Accelerate à votre CloudTrail compte ou à votre historique d'organisation.

Passez en revue les configurations de vos CloudTrail sentiers, la politique relative aux compartiments Amazon S3 et les politiques AWS KMS clés relatives à la destination de diffusion de vos CloudTrail événements avec votre architecte cloud (CA)

Avant qu'Accelerate puisse utiliser CloudTrail votre historique, vous devez travailler avec votre architecte cloud (CA) pour revoir et mettre à jour vos configurations afin de répondre aux exigences d'Accelerate. Si vous choisissez d'intégrer Accelerate à votre historique d' CloudTrail organisation, votre autorité de certification travaille avec vous pour mettre à jour le bucket Amazon S3 de destination de diffusion des CloudTrail événements et les politiques AWS KMS clés afin de permettre les requêtes entre comptes depuis votre compte Accelerate. Votre compartiment Amazon S3 peut se trouver dans un compte géré par Accelerate ou dans un compte que vous gérez. Pendant l'intégration, Accelerate vérifie que des requêtes peuvent être adressées à la destination de diffusion des événements de suivi de votre CloudTrail organisation, et suspend l'intégration si les requêtes échouent. Vous collaborez avec votre autorité de certification pour corriger ces configurations afin que l'intégration puisse reprendre.

Vérifiez et mettez à jour les configurations de suivi de votre CloudTrail compte ou de votre organisation

Les configurations suivantes sont requises pour intégrer la gestion accélérée des CloudTrail journaux à votre CloudTrail compte ou aux ressources de suivi de l'organisation :

- Votre CloudTrail parcours est configuré pour enregistrer les événements de tous Régions AWS.

- Les événements de service mondiaux sont activés sur votre CloudTrail parcours.
- Le journal de votre CloudTrail compte ou de votre organisation enregistre tous les événements de gestion, y compris les événements de lecture et d'écriture, AWS KMS et la journalisation des événements de l'API Amazon RDS Data est activée.
- La validation de l'intégrité du fichier journal est activée sur votre CloudTrail trace.
- Le compartiment Amazon S3 que vous suivez fournit CloudTrail des événements pour chiffrer les événements à l'aide du chiffrement SSE-S3 ou SSE-KMS.
- La journalisation des accès au serveur est activée dans le compartiment Amazon S3 auquel votre CloudTrail trace envoie un événement.
- Le compartiment Amazon S3 auquel votre CloudTrail trace envoie un événement possède une configuration de cycle de vie qui conserve les données de votre CloudTrail trace pendant au moins 18 mois.
- La propriété de l'objet définie sur le propriétaire du compartiment (bucket owner) est appliquée au bucket (propriétaire du compartiment) Amazon S3 vers lequel votre CloudTrail trace envoie un événement.
- Le compartiment Amazon S3 auquel votre CloudTrail trace envoie un événement est accessible par Accelerate.

Passez en revue et mettez à jour la politique relative aux compartiments Amazon S3 pour la destination de diffusion de vos CloudTrail événements

Lors de l'intégration, vous collaborez avec votre architecte cloud (CA) pour ajouter les déclarations de politique relatives aux compartiments Amazon S3 à la destination de diffusion de vos CloudTrail événements. Pour permettre à vos utilisateurs de demander des modifications dans le compartiment Amazon S3 de destination de diffusion de vos CloudTrail événements depuis votre compte Accelerate, vous pouvez déployer un rôle IAM portant le même nom dans chaque compte de votre organisation géré par Accelerate, et l'ajouter à la `aws:PrincipalArn` liste figurant dans toutes les déclarations de politique relatives aux compartiments Amazon S3. Grâce à cette configuration, vos utilisateurs peuvent interroger et analyser les événements de suivi de CloudTrail l'organisation de votre compte dans Accelerate using Athena. Pour plus d'informations sur la mise à jour d'une politique de compartiment Amazon S3, consultez Ajouter une politique de compartiment à l'aide de la console Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Important

La mise à jour de votre politique de compartiment Amazon S3 n'est requise que lorsque Accelerate s'intègre à un CloudTrail journal qui transmet les événements à un compartiment S3 centralisé. Accelerate ne prend pas en charge l'intégration à un CloudTrail suivi qui livre vers un compartiment centralisé mais qui ne possède pas les comptes d'une AWS organisation.

Note

Avant de mettre à jour votre politique relative aux compartiments Amazon S3, remplacez *red* les champs par les valeurs applicables :

- *amzn-s3-demo-bucket*avec le nom du compartiment Amazon S3 qui contient les événements de suivi de vos comptes.
- *your-organization-id*avec l'identifiant de l' AWS organisation dont vos comptes sont membres.
- *your-optional-s3-log-delievery-prefix*avec le préfixe de livraison du compartiment Amazon S3 de votre CloudTrail parcours. Par exemple`my-bucket-prefix`, celui que vous avez peut-être défini lors de la création de votre CloudTrail parcours.

  Si vous n'avez pas configuré de préfixe de livraison de compartiment Amazon S3 pour votre parcours, supprimez « *your-optional-s3-log-delievery-prefix* » et la barre oblique (`/`) des déclarations de politique relatives aux compartiments Amazon S3 suivantes.

Les trois déclarations de politique relatives aux compartiments Amazon S3 suivantes accordent à Accelerate l'accès pour récupérer les configurations et exécuter des requêtes AWS Athena afin d'analyser les CloudTrail événements dans le compartiment Amazon S3 de destination de diffusion des événements à partir de votre compte Accelerate.

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWBUCKETCONFIGAUDIT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
```

```
    },
    "Action": [
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetEncryptionConfiguration"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
},
{
    "Sid": "DONOTDELETE-AMS-ALLOWLISTBUCKET",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringLike": {
            "s3:prefix": "your-optional-s3-log-delievery-prefix/AWSLogs/*"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
},
```

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWGETOBJECT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/your-optional-s3-log-delievery-
prefix/AWSLogs/*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
}
```

Passez en revue et mettez à jour la politique AWS KMS clé pour la destination de livraison de vos CloudTrail événements

Lors de l'intégration, vous collaborez avec votre architecte cloud (CA) pour mettre à jour la politique AWS KMS clé utilisée pour chiffrer les événements de CloudTrail suivi transmis à votre compartiment Amazon S3. Assurez-vous d'ajouter les déclarations de politique AWS KMS clés de référence à votre AWS KMS clé existante. Cela permet de configurer Accelerate pour l'intégrer à votre compartiment Amazon S3 CloudTrail de destination de diffusion d'événements de suivi existant et pour déchiffrer les événements. Pour permettre à vos utilisateurs de demander des modifications dans le compartiment Amazon S3 de destination de diffusion de vos CloudTrail événements depuis votre compte Accelerate, vous pouvez déployer un rôle IAM portant le même nom dans chaque compte de votre organisation géré par Accelerate, et l'ajouter à la liste « aws : PrincipalArn ». Avec cette configuration, vos utilisateurs peuvent interroger les événements.

Il existe différents scénarios AWS KMS clés de mise à jour des politiques à envisager. Il se peut que vous n'ayez configuré qu'une AWS KMS clé pour votre CloudTrail parcours afin de chiffrer tous les événements, et qu'aucune AWS KMS clé ne chiffre les objets de votre compartiment Amazon S3.

Vous pouvez également avoir une AWS KMS clé qui chiffre les événements transmis par CloudTrail, et une autre AWS KMS clé qui chiffre tous les objets stockés dans votre compartiment Amazon S3. Lorsque vous disposez de deux AWS KMS clés, vous mettez à jour la politique AWS KMS clé pour chaque clé afin d'autoriser Accelerate à accéder à vos CloudTrail événements. Assurez-vous de modifier la déclaration de politique AWS KMS clé de référence par rapport à votre politique AWS KMS clé existante avant de mettre à jour la politique. Pour plus d'informations sur la mise à jour d'une politique AWS KMS clé, consultez la section Modification d'une politique clé dans le Guide de AWS Key Management Service l'utilisateur.

Important

Vous êtes tenu de mettre à jour votre politique en matière de AWS KMS clés uniquement lorsque Accelerate s'intègre à un journal CloudTrail avec le chiffrement SSE-KMS des fichiers journaux activé.

Note

Avant d'appliquer cette déclaration de politique AWS KMS clé à la AWS KMS clé utilisée pour chiffrer vos AWS CloudTrail événements transmis à votre compartiment Amazon S3, remplacez les *red* champs suivants par les valeurs applicables :

- *YOUR-ORGANIZATION-ID*avec l'identifiant de l' AWS organisation dont vos comptes sont membres.

Cette déclaration de politique AWS KMS clé accorde à Accelerate l'accès au déchiffrement et à l'interrogation des événements transmis au compartiment Amazon S3 à partir de chaque compte de votre organisation avec un accès restreint à Athena, utilisée par Accelerate pour interroger et CloudTrail analyser les événements. .

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWTRAILOBJECTDECRYPTION",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Decrypt",
```

```
            "kms:DescribeKey"
        ],
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:CalledVia": "athena.amazonaws.com"
            },
            "StringEquals": {
                "aws:PrincipalOrgID": "YOUR-ORGANIZATION-ID"
            },
            "ArnLike": {
                "aws:PrincipalArn": [
                    "arn:aws:iam::*:role/ams-access-*"
                ]
            }
        }
}
```

Le modèle pour créer des rôles AMS

Le rôle AMS suivant accorde des autorisations à votre architecte cloud AMS (CA). Le fichier zip suivant contient du code Terraform et un AWS CloudFormation modèle qui simplifient la création du rôle IAM, de la politique d'autorisation et de la politique de confiance. Pour plus d'informations, contactez votre autorité de certification.

Nom du rôle	Requis par	Exemples de modèles
`aws_managedservices_onboarding_role`	Personnel AMS uniquement lors de l'intégration	onboarding_role_minimal.zip

> **Note**
>
> Après avoir sélectionné et téléchargé un exemple de modèle (un par rôle), vous le téléchargerez sous forme de définitions de AWS CloudFormation piles dansCréez `aws_managedservices_onboarding_role` avec AWS CloudFormation for Accelerate.

Créez **aws_managedservices_onboarding_role** avec AWS CloudFormation for Accelerate

Vous pouvez créer le AWS Identity and Access Management rôle`aws_managedservices_onboarding_role`, à AWS CloudFormation partir du AWS Management Console. Vous pouvez également utiliser les commandes de AWS CloudShell pour déployer le rôle.

Utilisez le AWS Management Console

> **Note**
>
> Avant de commencer, préparez un fichier JSON ou YAML pour chaque rôle, prêt à être chargé. Pour de plus amples informations, veuillez consulter Le modèle pour créer des rôles AMS.

Pour créer le rôle à partir du AWS Management Console, procédez comme suit :

1. Connectez-vous à la AWS CloudFormation console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudformation.

2. Choisissez Create Stack > Avec de nouvelles ressources (standard). La page suivante s'affiche.

3. Choisissez Télécharger un fichier modèle, chargez le fichier JSON ou YAML du rôle IAM, puis choisissez Next. La page suivante s'affiche.

4. Entrez le nom de la pile « **ams-onboarding-role** » dans le champ Nom de la pile. Entrez un DateOfExpiryen utilisant le format « YYYY-MM-DDT 00:00:00 Z » (30 jours à compter de la date actuelle sont recommandés). Continuez à faire défiler l'écran vers le bas et à sélectionner Suivant jusqu'à ce que vous atteigniez cette page :

5. Assurez-vous que la case est cochée, puis sélectionnez Create Stack.
6. Assurez-vous que la pile a été créée avec succès.

Utilisez les commandes de AWS CloudShell

Pour déployer le rôle `aws_managedservices_onboarding_role` IAM, exécutez la commande suivante dans AWS CloudShell:

AWS CLI

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/onboarding_role_minimal.zip" -o "onboarding_role_minimal.zip"
unzip -q -o onboarding_role_minimal.zip
aws cloudformation create-stack \
    --stack-name "aws-managedservices-onboarding-role" \
    --capabilities CAPABILITY_NAMED_IAM \
    --template-body file://onboarding_role_minimal.json \
    --parameters ParameterKey=DateOfExpiry,ParameterValue="`date -d '+30 days' -u '+
%Y-%m-%dT%H:%M:%SZ'`"
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/
latest/accelerate-guide/samples/onboarding_role_minimal.zip' -OutFile
 'onboarding_role_minimal.zip'
Expand-Archive -Path 'onboarding_role_minimal.zip' -DestinationPath . -Force
New-CFNStack `
    -StackName 'aws-managedservices-onboarding-role' `
    -Capability CAPABILITY_NAMED_IAM `
    -TemplateBody (Get-Content 'onboarding_role_minimal.json' -Raw) `
    -Parameter @{ParameterKey = "DateOfExpiry"; ParameterValue = (Get-
Date).AddDays(30).ToString('yyyy-MM-ddTHH:mm:ssZ')}
```

Après avoir créé le rôle, collaborez avec votre architecte cloud (CA) pour terminer le Étape 2. Ressources de gestion de l'intégration dans Accelerate processus. Une fois qu'AMS vous a informé que votre compte est actif, vous êtes prêt à intégrer vos instances.

Étape 3. Intégration des fonctionnalités AMS avec des politiques par défaut

À ce stade, vous intégrez les fonctionnalités AMS avec des politiques par défaut. Cela inclut l'ajout d' EC2 instances Amazon et la configuration de la surveillance, de la sauvegarde, de AWS Config la correction et des correctifs (le cas échéant, AMS Patch Orchestrator est un module complémentaire que vous devez spécifiquement demander) selon vos préférences. Vous pouvez le faire vous-

même ou demander à AMS d'intégrer des fonctionnalités en fonction de vos informations. Pour demander de l'aide à AMS, créez une demande de service et fournissez toutes les informations nécessaires pour terminer la tâche. N'oubliez pas que les demandes de service ne sont pas résolues immédiatement.

> **Note**
>
> Bien qu'un compte puisse utiliser des politiques par défaut pour la sauvegarde, les correctifs ou la surveillance, les ressources doivent être balisées pour que la politique appropriée soit efficace.

Rubriques

- (Facultatif) Modèle de démarrage rapide dans Accelerate
- Intégration Accélérez la surveillance
- Intégrer des EC2 instances pour accélérer
- Intégration à AWS Backup Accelerate
- Intégration des correctifs dans Accelerate
- Consultez les rapports de non-conformité dans Accelerate

(Facultatif) Modèle de démarrage rapide dans Accelerate

Le modèle Quick Start automatise le déploiement et la configuration d'AMS Resource Tagger dans les comptes compatibles AWS Accelerate. Ce modèle permet d'économiser du temps et des efforts par rapport à une configuration manuelle. Utilisez ce modèle tel quel pour définir les principes de base de la surveillance, de l'application de correctifs et de la sauvegarde dans un seul compte. Vous pouvez également l'utiliser StackSet pour appliquer des paramètres à toutes les unités d'organisations afin de standardiser les paramètres de plusieurs comptes.

Vous pouvez également l'utiliser comme point de départ pour créer votre propre profil AMS Resource Tagger personnalisé et utiliser des extraits de la documentation pour créer des définitions plus complexes pour le balisage.

Fonctionnalité du modèle Quick Start

Le modèle Quick Start exécute les tâches suivantes :

- Crée et déploie une version de configuration pour AMS Resource Tagger.

- Applique des balises aux EC2 instances Amazon qui permettent la gestion AMS et la création de ressources de surveillance.
- (Facultatif) Applique des balises aux EC2 instances gérées qui permettent de leur appliquer des correctifs selon le calendrier souhaité, et crée une fenêtre de maintenance des correctifs pour faciliter l'application des correctifs.

  > **Warning**
  >
  > Par défaut, les instances sont redémarrées et les instances arrêtées sont démarrées automatiquement pour l'installation des correctifs.

- (Facultatif) Applique des balises aux EC2 instances gérées qui permettent de les sauvegarder comme défini dans le plan de sauvegarde AMS par défaut.
- (Facultatif) Applique des balises aux ressources gérées par Amazon Relational Database Service (Amazon RDS) afin de les sauvegarder conformément au plan de sauvegarde amélioré. Un plan de sauvegarde permet également la restauration ponctuelle (PITR) pour Amazon RDS. Si la sauvegarde automatique Amazon RDS n'est pas activée, la base de données redémarre à peu près au moment de la fenêtre de sauvegarde suivante.

Dérogations et exclusions du modèle Quick Start

Après avoir utilisé ce modèle pour créer une pile Quick Start, suivez les étapes suivantes pour exclure des instances spécifiques de Management/Monitoring, Patching ou Backup :

- Gestion et surveillance : pour exclure une EC2 instance de la gestion et de la surveillance par AMS, ajoutez cette balise à l'instance :`ExcludeFromAMSQuickStartMonitoring=true`.
- Application de correctifs : les EC2 instances membres d'un groupe Auto Scaling, d'Amazon Elastic Container Service ou d'un cluster Amazon Elastic Kubernetes Service sont exclues de l'application de correctifs par ce modèle de démarrage rapide.

  Pour désactiver la création d'une fenêtre de correction et le balisage des EC2 instances lié aux correctifs, définissez le CloudFormation paramètre de pile sur. `EnablePatching=false`

  Pour empêcher une EC2 instance d'être ciblée par la fenêtre d'application de correctifs Quick Start à quel moment`EnablePatching=true`, ajoutez cette balise à l'instance :`ExcludeFromAMSQuickStartPatching=true`.

- Backup : les EC2 instances membres d'un groupe Auto Scaling, d'un cluster ECS ou d'un cluster EKS sont exclues de la sauvegarde par ce modèle Quick Start.

  Pour exclure une EC2 instance de la cible du plan de sauvegarde AMS par défaut, quand`EnableBackup=true`, ajoutez cette balise à cette instance :`ExcludeFromAMSQuickStartBackup=true`.

> **Tip**
>
> Vous pouvez étiqueter EC2 des instances en bloc. Utilisez l'éditeur de balises pour sélectionner et étiqueter en bloc les ressources en une seule étape dans le. AWS Management Console

Paramètres du modèle Quick Start

Ce modèle Quick Start configure Resource Tagger pour ajouter le tag `ams:rt:ams-managed=true` à toutes les EC2 instances du compte, à l'exception des instances auxquelles vous ajoutez le `ExcludeFromAMSQuickStartMonitoring=true` tag. Utilisez les paramètres suivants pour contrôler les parties facultatives de cette pile en fonction de vos besoins :

Paramètre CFN	Valeur	Effet
EnableBackup	« vrai » (par défaut)	Toutes les EC2 instances gérées par AMS (`ams:rt:ams-managed =true`) sont étiquetées `ams:rt:ba ckup-orchestrator=true` pour être sauvegardées quotidien nement à 4 h UTC, conformément au plan de sauvegarde AMS par défaut. Pour toutes les instances et clusters RDS, le modèle applique la `ams:rt:backup-orch estrator-enhanced=true` « sauvegarde continue » avec une rétention maximale (31 jours)

Paramètre CFN	Valeur	Effet
		conformément au plan de sauvegarde amélioré. Si cela modifie votre période de conservation du PITR, la base de données peut être redémarrée dans certains cas, par exemple si d'autres mises à jour de configuration sont en attente.
	'fausse'	Aucune instance n'est ciblée pour la sauvegarde par ce modèle de démarrage rapide.
EnablePatching	« faux » (par défaut)	Aucune instance n'est ciblée pour l'application de correctifs par ce modèle de démarrage rapide.
	'vrai'	Toutes les instances gérées par AMS (`ams:rt:ams-managed=true`) sont étiquetées avec `ams:rt:Patch Group=AMSQuickStartPatchWindow` et une ressource de base de fenêtre de maintenance SSM est créée pour faciliter l'application des correctifs conformément au calendrier défini dans. `CronExpression` Pour appliquer la `ams:rt:Patch Group` balise à l' EC2 instance, vous devez désactiver l'accès aux balises dans les métadonnées de l'instance pour cette instance.

Paramètre CFN	Valeur	Effet
CronExpression	-	La valeur par défaut de `cron(0 30 19 ? * SAT#2 *)` définit le deuxième samedi du mois à 19 h 30 en fonction du `Timezone` paramètre. Utilisez la syntaxe cron.
Fuseau horaire	-	Les instances cibles sont patchées conformément à. `CronExpression` Utilisez le format IANA.

Téléchargez le modèle de démarrage rapide

Téléchargez le fichier AMSQuick Start.zip.

Vous pouvez également exécuter la commande suivante AWS CloudShellpour déployer `AMSQuickStart.yaml` :

AWS Command Line Interface

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/AMSQuickStart.zip" -o "AMSQuickStart.zip"
unzip -q -o AMSQuickStart.zip
for region in region1 region2 ;
do
aws cloudformation create-stack \
    --region $region \
    --stack-name "AMSQuickStart" \
    --template-body file://AMSQuickStart.yaml \
    --parameters \
        ParameterKey=EnableBackup,ParameterValue="true" \
        ParameterKey=EnablePatching,ParameterValue="false" \
        ParameterKey=Timezone,ParameterValue="US/Eastern" \
        ParameterKey=CronExpression,ParameterValue="cron(0 30 19 ? * SAT#2 *)" \
;
done
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/latest/
accelerate-guide/samples/AMSQuickStart.zip' -OutFile 'AMSQuickStart.zip'
Expand-Archive -Path 'AMSQuickStart.zip' -DestinationPath . -Force
@('region1', 'region2') | `
ForEach-Object { `
New-CFNStack `
    -Region $_ `
    -StackName 'AMSQuickStart' `
    -TemplateBody (Get-Content 'AMSQuickStart.yaml' -Raw) `
    -Parameter @(
        @{ParameterKey = "EnableBackup"; ParameterValue = "true"},
        @{ParameterKey = "EnablePatching"; ParameterValue = "false"},
        @{ParameterKey = "Timezone"; ParameterValue = "US/Eastern"},
        @{ParameterKey = "CronExpression"; ParameterValue = "cron(0 30 19 ? * SAT#2
 *)"}
    )
}
```

Pour une description de chaque paramètre, reportez-vous à la section précédente,Paramètres du modèle Quick Start.

Intégration Accélérez la surveillance

La surveillance est activée par défaut pour toutes les nouvelles ressources, à l'exception des EC2 instances Amazon. Vous pouvez commencer à surveiller vos EC2 instances Amazon en les étiquetant.

Pour intégrer la surveillance, assurez-vous d'abord que votre configuration surveille les ressources que vous souhaitez qu'AMS surveille et ignore les ressources que vous souhaitez qu'il ignore.

Vous pouvez utiliser les CloudWatch tableaux de bord suivants pour savoir combien de vos ressources sont ciblées par la surveillance et le balisage AMS, et combien ne le sont pas. Dans votre compte, accédez à la console CloudWatch des tableaux de bord et sélectionnez l'une des options suivantes :

- Tableau de bord de rapports AMS-Alarm-Manager-
- Tableau de bord de rapports AMS-Resource Tagger

Pour une description complète des statistiques du tableau de bord, voir :

- Affichage du nombre de ressources surveillées par Alarm Manager pour Accelerate
- Afficher le nombre de ressources gérées par Resource Tagger

Ressources d'intégration à surveiller dans Accelerate

Pour modifier le comportement par défaut, par exemple pour désactiver la surveillance par défaut pour les ressources autres que les EC2 ressources, vous devez supprimer le balisage de ces ressources à l'aide d'un profil de configuration personnalisé. Pour plus d'informations sur le balisage à des fins de surveillance, consultezSurveillance dans Accelerate.

La surveillance est désactivée pour les EC2 instances jusqu'à ce que vous les intégriez, ce qui inclut le balisage de vos instances à l'aide d'un profil de configuration personnalisé. La section suivante décrit l'intégration des EC2 instances.

Création d'un profil de configuration de surveillance dans Accelerate

- Pour plus d'informations sur l'utilisation de la configuration par défaut, consultezAccélérer Alarm Manager.
- Pour plus d'informations sur l'utilisation d'une configuration personnalisée, consultezModification de la configuration par défaut de l'alarme Accelerate.

Intégrer des EC2 instances pour accélérer

EC2 les instances sont intégrées à AMS Accelerate par le biais d'un processus appelé Configuration automatisée des instances, qui garantit que chaque instance écrit les bons journaux et émet les mesures appropriées pour qu'AMS puisse gérer correctement l'instance. Vous devez intégrer toutes vos EC2 instances, sauf si vous souhaitez spécifiquement qu'AMS en ignore certaines. La configuration d'instance automatisée nécessite le respect de conditions spécifiques permettant à AMS de configurer l'instance (pour plus de détails, voirConditions préalables à la configuration automatique des instances dans Accelerate). La condition la plus importante est que l' AWS Systems Manager agent (agent SSM) doit être installé sur chaque EC2 instance Amazon que vous souhaitez qu'AMS gère pour vous. Pour plus d'informations sur l'agent SSM, consultez la section Utilisation de l'agent SSM.

SSM préinstallé en standard AMIs pour Accelerate

L'agent SSM est déjà installé sur AWS-provided AMIs pour les systèmes d'exploitation suivants.

- Amazon Linux et Amazon Linux 2
- SUSE Linux Enterprise Server (SLES) 12 et 15
- Microsoft Windows Server 2019, 2016, 2012 R2, 2012
- Ubuntu Linux 18.04 et 20.04

Si vous utilisez l'un de ces outils AWS fournis AMIs, consultezMarquer des instances dans Accelerate.

Installation manuelle de SSM dans Accelerate

Pour les systèmes d'exploitation suivants, ou lorsque vous utilisez une AMI personnalisée, vous pouvez installer manuellement l'agent SSM. Vous pouvez également utiliser la fonction d'installation automatique de l'agent AMS SSM. Pour en savoir plus sur l'installation automatique de SSM, consultezInstallation automatique de l'agent SSM. Pour obtenir des instructions sur l'installation manuelle, sélectionnez le lien correspondant à votre système d'exploitation :

- Installation de CentOS SSM
- Installation d'Oracle SSM
- Installation de Red Hat SSM
- Installation de SUSE Linux Enterprise Server SSM
- Installation de Windows SSM

Marquer des instances dans Accelerate

Une fois l'agent SSM installé, vous devez étiqueter vos instances. Consultez Marquage dans AMS Accelerate.

Configuration d'instance automatisée dans Accelerate

Une fois que votre instance est étiquetée, AMS effectue une configuration d'instance automatisée, qui inclut :

- Enregistrer les journaux et les indicateurs du système d'exploitation
- Permettre l'accès à distance pour les ingénieurs AMS
- Exécuter des commandes à distance sur l'instance

Ces tâches sont essentielles pour les services de surveillance, de correction et de journalisation d'AMS, ainsi que pour permettre à AMS de répondre aux incidents. Pour plus de détails sur la configuration de la configuration automatique des instances, consultezConfiguration d'instance automatisée dans AMS Accelerate.

Une fois la configuration automatique de l'instance terminée, vous pouvez :

- Créez des incidents et des demandes de service pour les EC2 instances Amazon et les systèmes d'exploitation à l'aide de la console Support Center. Pour de plus amples informations, veuillez consulter Rapports d'incidents, demandes de service et questions de facturation dans AMS Accelerate.
- Accédez aux EC2 journaux Amazon et auditez-les
- Obtenir des rapports sur les correctifs

Intégration à AWS Backup Accelerate

Pour configurer les sauvegardes, vous devez créer des politiques de sauvegarde appelées plans de sauvegarde. Un plan de sauvegarde indique les AWS ressources à sauvegarder, la fréquence à laquelle elles doivent être sauvegardées et la période de conservation des sauvegardes. Nous vous recommandons d'évaluer les exigences de continuité, de sécurité et de conformité de votre organisation afin de déterminer les plans de sauvegarde dont vous avez besoin.

S'inscrire

- Assurez-vous que cette option AWS Backup est activée pour chaque compte, région et type de ressource en suivant les étapes ci-dessous :

  Mise en route 1 : Inscription au service.

  Facultativement, Mise en route 2 : création sur sauvegarde à la demande.

Choisissez un plan de sauvegarde

- Pour choisir un plan de sauvegarde, voirSélectionnez un plan de sauvegarde AMS.

Ajouter des ressources

Les ressources ne sont pas associées à un plan de sauvegarde par défaut. Ils doivent être ajoutés à un plan de sauvegarde.

- Pour ajouter des ressources à un plan de sauvegarde, voirÉtiquetez vos ressources pour appliquer les plans de sauvegarde AMS.
- Pour activer la sauvegarde de toutes les ressources à l'aide de balises, voirGestion des balises pour les sauvegardes dans Accelerate.

Intégration des correctifs dans Accelerate

Vous devez configurer les correctifs pour vous assurer que votre logiciel est up-to-date conforme à vos politiques de conformité.

AWS Backup condition préalable : pour autoriser la création d'un instantané du volume racine pendant la période de maintenance des correctifs, assurez-vous qu'il AWS Backup est activé pour chaque compte et région pour le type de ressource Amazon EBS en suivant les étapes ci-dessous : Démarrage 1 : Service Opt-in. (Il n'est pas nécessaire de passer à la section Mise en route 2 : création d'une sauvegarde à la demande.)

Quand appliquer un correctif : l'application de correctifs a lieu pendant une fenêtre de maintenance. Vous pouvez planifier des fenêtres de maintenance de manière à ce que les correctifs ne soient appliqués que pendant des périodes prédéfinies.

Éléments à corriger : vous devez associer les EC2 instances Amazon que vous souhaitez patcher à une fenêtre de maintenance. Pour associer les instances à une fenêtre de maintenance, les EC2 instances Amazon doivent être étiquetées, et la fenêtre de maintenance doit avoir ces balises comme cible.

Quels correctifs installer : à l'aide des lignes de base des correctifs, vous définissez des règles pour approuver automatiquement certains types de correctifs, tels que les correctifs de système d'exploitation ou les correctifs de gravité élevée. Vous pouvez également spécifier des exceptions à vos règles, par exemple des listes de correctifs qui sont toujours approuvés ou rejetés.

Consultez Recommandations relatives aux correctifs pour obtenir des conseils sur les politiques relatives aux EC2 correctifs d'Amazon.

- Pour commencer à configurer la gestion des correctifs, voir Comprendre la gestion des correctifs dans AMS Accelerate

- Pour créer une configuration de correctif personnalisée, voirBase de correctifs personnalisée avec AMS Accelerate.

Consultez les rapports de non-conformité dans Accelerate

AMS déploie des AWS Config règles qui vous aident à identifier les violations des normes établies par le Center for Internet Security (CIS) et le cadre de sécurité cloud (CSF) du National Institute of Standards and Technology (NIST). Nous vous recommandons de consulter le rapport de non-conformité avec votre équipe de livraison afin de hiérarchiser les mesures correctives afin que votre compte soit redéfini comme étant conforme.

Étape 4 : Personnalisez les fonctionnalités dans Accelerate

À ce stade, vous avez déjà intégré la surveillance, l'application de correctifs et la sauvegarde avec des politiques par défaut. Vous avez désormais la possibilité de personnaliser les politiques en fonction de vos besoins.

Vous pouvez choisir d'utiliser les politiques par défaut pour les correctifs, les sauvegardes ou la surveillance, ou de choisir une politique personnalisée en fonction de vos besoins. AMS utilise des balises pour associer les ressources aux politiques opérationnelles. AMS fournit un tagger de ressources qui vous permet de définir des règles sur la manière dont les balises sont appliquées à vos AWS ressources en fonction du regroupement d'applications ou d'une autre logique de regroupement. Pour plus d'informations, consultezAccélérez Resource Tagger.

La fonctionnalité de balises fournies par le client vous permet d'ajouter et de supprimer des balises personnalisées aux ressources AMS. Pour de plus amples informations, veuillez consulter Tags fournis par le client dans Accelerate.

Rubriques

- Personnalisez la surveillance dans Accelerate
- Personnalisez la sauvegarde dans Accelerate
- Personnaliser l'application de correctifs dans Accelerate

Personnalisez la surveillance dans Accelerate

Pour personnaliser la surveillance de vos ressources cloud en fonction des besoins de vos applications :

1. Créez une politique de surveillance personnalisée. Consultez Modification de la configuration par défaut de l'alarme Accelerate.
2. Appliquez une politique personnalisée aux ressources à l'aide de balises. Consultez Surveillance dans Accelerate.
3. Acheminez les alertes vers le propriétaire de la ressource. Consultez Notification d'alerte basée sur des balises.

Vous pouvez utiliser les CloudWatch tableaux de bord suivants pour savoir combien de vos ressources sont ciblées par la surveillance et le balisage AMS, et combien ne le sont pas. Dans votre compte, accédez à la console CloudWatch des tableaux de bord et sélectionnez l'une des options suivantes :

- Tableau de bord de rapports AMS-Alarm-Manager-
- Tableau de bord de rapports AMS-Resource Tagger

Pour une description complète des statistiques du tableau de bord, voir :

- Affichage du nombre de ressources surveillées par Alarm Manager pour Accelerate
- Afficher le nombre de ressources gérées par Resource Tagger

Personnalisez la sauvegarde dans Accelerate

Vous ne pouvez pas personnaliser les plans de sauvegarde par défaut d'AMS. Créez plutôt un nouveau plan de sauvegarde en fonction des besoins de votre application, puis associez des ressources à votre plan personnalisé à l'aide de balises. C'est à vous de choisir les ressources qu'AMS doit sauvegarder, à quelle fréquence et pendant quelle période de conservation. Nous vous recommandons d'évaluer les exigences de continuité, de sécurité et de conformité de votre organisation afin de déterminer les plans de sauvegarde dont vous avez besoin.

- Pour créer un plan de sauvegarde, voir Création d'un plan de sauvegarde.
- Pour affecter des ressources à un plan de sauvegarde, voir Affecter des ressources à un plan de sauvegarde.

Personnaliser l'application de correctifs dans Accelerate

L'application de correctifs garantit que votre logiciel est conforme up-to-date à vos politiques de conformité.

Quand appliquer un correctif : l'application de correctifs a lieu pendant une fenêtre de maintenance. Vous pouvez planifier des fenêtres de maintenance de manière à ce que les correctifs ne soient appliqués que pendant des périodes prédéfinies.

Éléments à corriger : vous devez associer les EC2 instances Amazon que vous souhaitez patcher à une fenêtre de maintenance. Pour associer les instances à une fenêtre de maintenance, les EC2 instances Amazon doivent être étiquetées, et la fenêtre de maintenance doit avoir ces balises comme cible.

Quels correctifs installer : à l'aide des lignes de base des correctifs, vous définissez des règles pour approuver automatiquement certains types de correctifs, tels que les correctifs de système d'exploitation ou les correctifs de gravité élevée. Vous pouvez également spécifier des exceptions à vos règles, par exemple des listes de correctifs qui sont toujours approuvés ou rejetés.

- Pour les recommandations générales relatives aux correctifs, voirRecommandations relatives aux correctifs.
- Pour créer des fenêtres de maintenance personnalisées, voirCréation d'une fenêtre de maintenance des correctifs dans AMS.
- Pour créer des lignes de base de correctifs personnalisées, voirBase de correctifs personnalisée avec AMS Accelerate.
- Pour acheminer les alertes de correctifs vers le propriétaire de la ressource, consultezComprendre les notifications relatives aux correctifs et les défaillances des correctifs dans AMS Accelerate.

Utilisation des consoles AMS

Les consoles AMS de la console AWS de gestion vous permettent d'interagir avec AMS et d'exploiter vos ressources gérées par AMS Advanced et AMS Accelerate. Les consoles AMS se comportent généralement comme n'importe quelle AWS console ; toutefois, comme AMS est une organisation privée, seuls les comptes activés pour AMS peuvent accéder à la console. Une fois AMS activé dans votre compte, vous pouvez accéder à la console en recherchant « Managed Services » dans la barre de recherche unifiée.

> **Note**
>
> Selon le rôle de votre compte, vous accédez à la console AMS Advanced ou à la console AMS Accelerate.

Lorsque vous utilisez les consoles AMS, tenez compte des mises en garde suivantes :

- La console AMS est spécifique au compte. Ainsi, si vous utilisez un compte « Test » pour votre organisation, vous ne pourrez pas voir les ressources du compte « Prod » de cette organisation. De même, vous devez disposer d'un rôle AMS Advanced pour accéder à la console AMS Advanced.
- Les consoles AMS appliquent une politique IAM lors de l'authentification qui détermine à quelle console vous pouvez accéder et ce que vous pouvez y faire. Votre administrateur peut appliquer des politiques supplémentaires à la politique AMS par défaut afin de limiter ce que vous pouvez voir et faire dans la console.

La console AMS Accelerate possède les fonctionnalités suivantes :

- Page d'ouverture : La page d'ouverture contient des boîtes d'information et des liens pour faciliter votre accès à vos incidents à vos demandes de service et à vos rapports.
- Pages de fonctionnalités, liens dans le volet de navigation de gauche :
  - Tableau de bord : fournit un aperçu de l'état actuel de votre compte, notamment :
    - Incidents affectant vos ressources : bouton permettant d'ouvrir un dossier d'incident dans le centre de support AWS, ainsi que le nombre de cas d'incidents en attente d'approbation qui nécessitent votre attention et le nombre de cas ouverts
    - État de conformité : liens vers des règles et des ressources non conformes ou conformes
    - Demandes de service : bouton permettant d'ouvrir un dossier de demande de service dans le centre de support AWS, ainsi que le nombre de demandes en attente d'approbation nécessitant votre attention et le nombre de demandes ouvertes
    - Sécurité au niveau du compte : liens vers des informations sur les résultats de détection des menaces en temps réel et sur GuardDuty les résultats de Macie relatifs à la sécurité et à la confidentialité des données
    - Actions rapides : ouvrez les pages de configuration de vos coffres-forts de sauvegarde ou de vos instances de correctifs

- Rapports : ouvre la page des rapports et les rapports par défaut, Daily Backup, Daily Patch et Monthly Facturation
- Configuration : assurez-vous que vos ressources sont gérées correctement et conformément à vos spécifications.
  - Installation de l'agent SSM : l'agent SSM est requis
  - Configurer les règles de balisage : ouvre AMS Resource Tagger
  - Configurer les alarmes : ouvre la configuration des CloudWatch alarmes AMS
  - Configurer le calendrier des correctifs : ouvre la console AWS Systems Manager
  - Configurer les lignes de base des correctifs : ouvre la console AWS Patch Manager
  - Configuration des plans de sauvegarde : ouvre la console AWS Backup
- Présentation des fonctionnalités : informations sur les dernières mises à jour de la console
- Documentation : page d'accueil de la documentation d'AWS Managed Services

Motifs AMS

Un modèle AWS Managed Services (AMS) est une solution généralisée qui permet de résoudre une famille de cas d'utilisation dans l'environnement géré AMS.

Lorsque vous travaillez sur la plateforme AMS, les architectes cloud AMS (CAs) travaillent avec vous pour répondre à vos exigences commerciales et opérationnelles. Bien que les clients d'AMS opèrent de manière unique, nous remarquons que les clients ont des cas d'utilisation similaires. Dans de tels cas, CAs créez des modèles de solution généraux, ou « modèles », qui sont utilisés dans plusieurs environnements clients avec un minimum d'efforts de configuration et de déploiement.

Les modèles AMS sont conçus pour aider à fournir des fonctionnalités aux clients AMS et sont généralement créés par l'autorité de certification du compte du client qui en fait la demande.

Comment fonctionnent les modèles AMS

Pour demander plus de détails sur chaque modèle, y compris les modèles de formation sur le cloud nécessaires au déploiement du modèle, soumettez une demande de service AMS avec pour objet « Demande de détails supplémentaires sur le modèle *`Pattern_Name`* » (remplacez le modèle que vous souhaitez) et ajoutez votre architecte de cloud AMS (CA) à l'option Contacts supplémentaires.

Les modèles AMS sont classés en deux (2) catégories :

- Utilisation générale : Les modèles sont considérés comme stables car ils ont été déployés et utilisés par plusieurs clients AMS
- Mode de prévisualisation : AMS recommande de déployer des modèles de mode de prévisualisation dans vos environnements hors production à des fins de validation, et de discuter avec votre architecte du cloud du cas d'utilisation avant le déploiement.

> **Important**
>
> Les modèles AMS ne respectent pas vos accords de niveau de service AMS par défaut, vos accords de niveau de service (SLAs) et vos objectifs de niveau de service (SLOs). Support et mises à jour du modèle sont effectués dans la mesure du possible.
> Ce AWS contenu est fourni conformément aux termes du contrat AWS client ou de tout autre accord écrit entre le client et Amazon Web Services, Inc. ou Amazon Web Services EMEA SARL (« AWS Europe ») ou les deux.
> Le matériel intégré dans ce logiciel vous est fourni « tel quel » et sans garantie d'aucune sorte, expresse, implicite ou autre, y compris, sans s'y limiter, toute garantie d'adéquation à un usage particulier.

Motifs AMS

Motifs AMS.

Motifs AMS

Name (Nom)	Présentation	Avantages	Catégorie
Personnaliser les notifications CloudWatch d'alarme	Personnalisez les notifications CloudWatch d'alarme pour inclure des informations provenant des balises d'instance telles que le nom de l'instance, l'ID de l'application, etc.	L'ajout d'informations contextuelles aux notifications d'alarme les rendra plus pertinentes et fournira des informations exploitables.	Surveillance

Name (Nom)	Présentation	Avantages	Catégorie
Rapports sur l'utilisation du disque	Le modèle de rapport sur l'utilisation du disque collecte l'espace de consommation des volumes sur plusieurs comptes d'applications et présente le résultat sous forme de rapport centralisé dans Amazon S3 avec fonction de requête de table Athena.	Fournissez des informations sur l'utilisation réelle des volumes de comptes afin de déterminer les opportunités de réduction des coûts.	Optimisation des coûts
Prowler Stack	Exécute des vérifications Prowler sur les comptes utilisant Amazon EC2 lorsqu'ils ne CloudShell peuvent pas être utilisés.	Aidez à débloquer l'intégration Accelerate (Prowler) dans les cas où il ne CloudShell peut pas être utilisé en raison d'autorisations ou de problèmes de délai d'attente, sans aucun impact sur leur niveau de sécurité actuel.	Sécurité

Name (Nom)	Présentation	Avantages	Catégorie
Réplication AMS Amazon S3 avec des clés d'objet personnalisées	Faites des copies des objets Amazon S3 et conservez toutes les métadonnées et clés d'objets (dossiers). Supprime une partie des clés de l'objet source ou crée des clés d'objet de destination personnalisées lors de la réplication.	Personnalisez les clés d'objet (dossiers) lors de la réplication Amazon S3 sans avoir besoin de scripts supplémentaires pour déplacer les objets vers les dossiers requis.	Fiabilité
Suppression d'un instantané Amazon EBS	Automatisation basée sur Lambda et CloudWatch Events pour automatiser la suppression des instantanés Amazon EBS pris en dehors de AWS Backup, sur la base de la rétention.	Aidez à purger les instantanés individuels pris en dehors de l' AWS Backup orchestrateur, réduisant ainsi les coûts supplémentaires au fil du temps.	Optimisation des coûts

Name (Nom)	Présentation	Avantages	Catégorie
Rotation des secrets d'AMS Amazon RDS	À l'aide d'un CloudFormation modèle, déployez automatiquement toutes les ressource s requises (fonction Lambda, groupes de sécurité, interfaces réseau élastiques ou ENIs) nécessaires à la rotation des secrets pour les bases de données Amazon RDS, Redshift et DocumentDB prises en charge.	Automatisez la rotation des secrets de base de données et fournissez un mécanisme de notification en cas d'échec de rotation.	Sécurité
Rotation automatique des clés	Faites automatiq uement pivoter les clés d'accès et les clés secrètes pour les utilisate urs IAM en fonction des CloudWatch événements et de Lambda.	Rotation facilitée des clés d'accès et des clés secrètes pour les utilisateurs IAM.	Sécurité

Name (Nom)	Présentation	Avantages	Catégorie
Étiqueteur d'instantanés de volume Amazon EBS	Marquez tous les volumes et instantanés Amazon EBS à l'aide des balises des instances Amazon EC2 .	Facilitez la catégorisation et le suivi des coûts grâce à des informations commerciales pertinentes et pertinentes, ce qui facilite la validation des dépenses, et autorisez l'automatisation des volumes étiquetés et des instantanés. Meilleure pratique hautement recommandée par le pilier de l'optimisation des AWS coûts.	Balisage (optimisation des coûts, sécurité, gestion des incidents et automatisation)

Configuration d'instance automatisée dans AMS Accelerate

AMS Accelerate fournit un service de configuration d'instance automatisé. Ce service garantit qu'une instance émet les journaux et les métriques appropriés pour qu'AMS puisse gérer correctement l'instance. La configuration automatique des instances comporte ses propres conditions préalables et étapes d'intégration, décrites plus loin dans cette section.

Rubriques

- Comment fonctionne la configuration automatique des instances dans Accelerate
- Installation automatique de l'agent SSM
- Modifications de configuration d'instance automatisées

Comment fonctionne la configuration automatique des instances dans Accelerate

La configuration automatique des instances permet à AMS Accelerate d'effectuer certaines configurations au quotidien sur des instances que vous indiquez en ajoutant des agents et des tags spécifiques.

Conditions préalables à la configuration automatique des instances dans Accelerate

Ces conditions doivent être remplies pour permettre à AMS Accelerate d'effectuer les actions automatisées décrites précédemment sur les instances gérées.

L'agent SSM est installé

La configuration automatique de l'instance AMS Accelerate nécessite l'installation de l'agent AWS Systems Manager SSM.

Pour plus d'informations sur l'utilisation de la fonctionnalité d'installation automatique de l'agent AMS SSM, voirInstallation automatique de l'agent SSM.

Pour plus d'informations sur l'installation manuelle de l'agent SSM, consultez les rubriques suivantes :

- Linux : installer manuellement l'agent SSM sur les EC2 instances Amazon pour Linux - AWS Systems Manager
- Windows : installez manuellement l'agent SSM sur les EC2 instances Amazon pour Windows Server - AWS Systems Manager

L'agent SSM est dans l'état géré

La configuration automatique des instances AMS Accelerate nécessite un agent SSM opérationnel. L'agent SSM doit être installé et l' EC2 instance Amazon doit être dans l'état géré. Pour plus d'informations, consultez la AWS documentation intitulée Utilisation de l'agent SSM.

Configuration automatique de la configuration des instances

En supposant que les conditions préalables soient remplies, l'ajout d'une balise d' EC2 instance Amazon spécifique lance automatiquement la configuration automatique de l'instance AMS Accelerate. Utilisez l'une des méthodes suivantes pour ajouter cette balise :

1. (Fortement recommandé) Utiliser le tagger de ressources AMS Accelerate

   Pour configurer la logique de balisage de votre compte, consultezComment fonctionne le balisage. Une fois le balisage terminé, les balises et la configuration automatique des instances sont gérées automatiquement.

2. Ajouter des tags manuellement

   Ajoutez manuellement la balise suivante aux EC2 instances Amazon :

   Clé : ams:rt:ams-managed, valeur : true.

> **Note**
>
> Le service de configuration d'instance tente d'appliquer les configurations AMS requises une fois que la balise ams:rt:ams-managed est appliquée à l'instance. Le service affirme les configurations requises par AMS chaque fois qu'une instance est démarrée et lors d'un contrôle de configuration quotidien de l'AMS.

Installation automatique de l'agent SSM

Pour qu'AMS gère vos instances Amazon Elastic Compute Cloud (Amazon EC2), vous devez installer l'agent AWS Systems Manager SSM sur chaque instance. Si l'agent SSM n'est pas installé sur vos instances, vous pouvez utiliser la fonction d'installation automatique de l'agent AMS SSM.

> **Note**
>
> - Si votre compte est intégré à AMS Accelerate après le 6 mars 2024, cette fonctionnalité est activée par défaut. Pour désactiver cette fonctionnalité, contactez votre autorité de certification ou votre CSDM.
> - Pour activer cette fonctionnalité dans les comptes intégrés avant le 6 mars 2024, contactez votre CA ou votre CSDM.
> - Cette fonctionnalité n'est disponible que pour les EC2 instances qui ne font pas partie d'un groupe Auto Scaling et qui exécutent des systèmes d'exploitation Linux pris en charge par AMS.

Conditions préalables à l'utilisation de l'agent SSM

- Assurez-vous que le profil d'instance associé aux instances cibles respecte l'une des politiques suivantes (ou des autorisations équivalentes à celles autorisées dans celles-ci) :
  - Amazon SSMManaged EC2 InstanceDefaultPolicy
  - Amazon SSMManaged InstanceCore
- Assurez-vous qu'il n'existe pas de politique de contrôle des services au AWS Organizations niveau qui refuse explicitement les autorisations répertoriées dans les politiques précédentes.

  Pour plus d'informations, consultez la section Configurer des autorisations d'instance requises pour Systems Manager.
- Pour bloquer le trafic sortant, assurez-vous que les points de terminaison d'interface suivants sont activés sur le VPC où résident les instances cibles (remplacez « région » dans l'URL de manière appropriée) :
  - ssm.<region>.amazonaws.com
  - ssmmessages.<region>.amazonaws.com
  - messages ec2. <region>.amazonaws.com

  Pour plus d'informations, consultez Améliorer la sécurité des EC2 instances en utilisant des points de terminaison VPC pour Systems Manager.

Pour obtenir des conseils généraux sur l'activation ou le dépannage de la disponibilité des nœuds gérés, voir Solution 2 : vérifier qu'un profil d'instance IAM a été spécifié pour l'instance (EC2 instances uniquement).

> **Note**
>
> AMS arrête et démarre chaque instance dans le cadre du processus d'installation automatique. Lorsqu'une instance est arrêtée, les données stockées dans les volumes de stockage de l'instance et les données stockées dans la RAM sont perdues. Pour plus d'informations, consultez Que se passe-t-il lorsque vous arrêtez une instance ?

Demandez l'installation automatique de l'agent SSM sur vos instances

Si vos comptes sont intégrés au module complémentaire AMS Accelerate Patch, configurez une fenêtre de maintenance des correctifs (MW) pour les instances. Un agent SSM fonctionnel est nécessaire pour terminer le processus de correction. Si l'agent SSM est absent d'une instance, AMS essaie de l'installer automatiquement pendant la fenêtre de maintenance des correctifs.

> **Note**
>
> AMS arrête et démarre chaque instance dans le cadre du processus d'installation automatique. Lorsqu'une instance est arrêtée, les données stockées dans les volumes de stockage de l'instance et les données stockées dans la RAM sont perdues. Pour plus d'informations, consultez Que se passe-t-il lorsque vous arrêtez une instance ?

Comment fonctionne l'installation automatique de l'agent SSM

AMS utilise les données EC2 utilisateur pour exécuter le script d'installation sur vos instances. Pour ajouter le script de données utilisateur et l'exécuter sur vos instances, AMS doit arrêter et démarrer chaque instance.

Si votre instance possède déjà un script de données utilisateur existant, AMS effectue les étapes suivantes au cours du processus d'installation automatique :

1. Crée une sauvegarde du script de données utilisateur existant.
2. Remplace le script de données utilisateur existant par le script d'installation de l'agent SSM.
3. Redémarre l'instance pour installer l'agent SSM.
4. Arrête l'instance et restaure le script d'origine.
5. Redémarre l'instance avec le script d'origine.

Modifications de configuration d'instance automatisées

L'automatisation de la configuration des instances AMS Accelerate apporte les modifications suivantes à votre compte :

1. Autorisations IAM

Ajoute les politiques gérées par IAM requises pour accorder à l'instance l'autorisation d'utiliser les agents installés par AMS Accelerate.

2. Agents
   a. L' CloudWatch agent Amazon est responsable de l'émission des journaux et des métriques du système d'exploitation. L'automatisation de la configuration de l'instance garantit que l' CloudWatch agent est installé et exécute la version minimale d'AMS Accelerate.
   b. L'agent AWS Systems Manager SSM est chargé d'exécuter les commandes à distance sur l'instance. L'automatisation de la configuration de l'instance garantit que l'agent SSM exécute la version minimale d'AMS Accelerate.
3. CloudWatch Configuration
   a. Pour garantir que les métriques et les journaux requis sont émis, AMS Accelerate personnalise la CloudWatch configuration. Pour plus d'informations, consultez la section suivante,CloudWatch détails des modifications de configuration.

La configuration automatique des instances apporte des modifications ou des ajouts aux profils et à la CloudWatch configuration de vos instances IAM.

Informations relatives à la modification des autorisations IAM

Chaque instance gérée doit avoir un AWS Identity and Access Management rôle qui inclut les politiques gérées suivantes :

- arn:aws:iam : :aws:policy/Amazon SSMManaged InstanceCore
- arn:aws:iam : :aws:policy/ CloudWatchAgentServerPolicy
- arn:aws:iam : :aws:policy/ AMSInstance ProfileBasePolicy

Les deux premières sont des politiques AWS gérées. La politique gérée par AMS est la suivante :

AMSInstanceProfileBasePolicy

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Action": [
                "secretsmanager:CreateSecret",
                "secretsmanager:UpdateSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:*:*:secret:/ams/byoa/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:Encrypt"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Si votre instance possède déjà un rôle IAM attaché, mais qu'aucune de ces politiques n'est absente, AMS ajoute les politiques manquantes à votre rôle IAM. Si votre instance ne possède pas de rôle IAM, AMS attache le rôle AMSOSConfigurationCustomerInstanceProfileIAM. Le rôle AMSOSConfigurationCustomerInstanceProfileIAM possède toutes les politiques requises par AMS Accelerate.

> **Note**
>
> Si la limite de 10 profils d'instance par défaut est atteinte, AMS augmente la limite à 20, afin que les profils d'instance requis puissent être attachés.

CloudWatch détails des modifications de configuration

Informations supplémentaires sur la CloudWatch configuration.

- CloudWatch emplacement du fichier de configuration sur l'instance :
  - Windows : % ProgramData % \ Amazon \ AmazonCloudWatchAgent \ amazon-cloudwatch-agent .json

    - Linux :/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/ams-accelerate-config.json
- CloudWatch emplacement du fichier de configuration dans Amazon S3 :
    - Windows : https ://ams-configuration-artifacts- *REGION_NAME* .s3. *REGION_NAME*.amazonaws. com/configurations/cloudwatch/latest/windows-cloudwatch-config.json
    - Linux : https ://ams-configuration-artifacts- *REGION_NAME* .s3. *REGION_NAME*.amazonaws. com/ configurations/cloudwatch/latest/linux-cloudwatch-config.json
- Métriques collectées :
    - Windows :
        - AWS Systems Manager Agent SSM (utilisation du processeur)
        - CloudWatch Agent (Utilisation du processeur)
        - Utilisation de l'espace disque pour tous les disques (% d'espace libre)
        - Mémoire (% d'octets engagés en cours d'utilisation)
    - Linux :
        - AWS Systems Manager Agent SSM (utilisation du processeur)
        - CloudWatch Agent (Utilisation du processeur)
        - Processeur (cpu_usage_idle, cpu_usage_iowait, cpu_usage_user, cpu_usage_system)
        - Disque (used_percent, inodes_used, inodes_total)
        - Diskio (io_time, write_bytes, read_bytes, écritures, lectures)
        - Mémoire (mem_used_percent)
        - Échange (swap_used_percent)
- Logs collectés :
    - Windows :
        - SSMAgentJournal Amazon
        - AmazonCloudWatchAgentLog
        - SSMErrorJournal Amazon
        - AmazonCloudFormationLog
        - ApplicationEventLog
        - EC2ConfigServiceEventLog
        - MicrosoftWindowsAppLockerEXEAndDLLEventJournal
        - MicrosoftWindowsAppLockerMSIAndScriptEventLog

    - MicrosoftWindowsGroupPolicyOperationalEventLog
    - SecurityEventLog
    - SystemEventLog
- Linux :
    - /var/log/amazon/ssm/amazon-ssm-agent.log
    - /var/log/amazon/ssm/errors.journal
    - /var/log/audit/audit.journal
    - /var/log/cloud-init-output.log
    - /var/log/cloud-init.log
    - /var/log/cron
    - /var/log/dpkg.journal
    - /var/log/maillog
    - /var/log/messages
    - /var/log/secure
    - /var/log/spooler
    - /var/log/syslog
    - /var/log/yum.journal
    - /var/log/zypper.journal

Déconnecter d'AMS Accelerate

AMS Accelerate fournit un moyen simple de gérer un environnement d'exploitation de niveau professionnel. De plus, AMS Accelerate fournit le modèle d'exploitation de l'infrastructure de support pour AWS la migration et l'utilisation. Cependant, après avoir utilisé AMS Accelerate, vous pouvez décider d'externaliser ou de réattribuer les responsabilités des opérations AWS d'infrastructure à d'autres équipes. Pour ce faire, vous devez déconnecter vos comptes du service AMS.

Lorsque vous déconnectez un compte d'AMS Accelerate, AMS vous transfère toutes les responsabilités définies dans la description de notre service. Par exemple, vous ne serez pas en mesure de réduire le nombre d'incidents ou de demandes de service adressés à AMS. De même, nos ingénieurs des opérations et de l'automatisation n'auront plus accès à vos comptes Accelerate, ce qui nous empêchera de remédier aux problèmes de santé, de disponibilité, de sécurité et de

conformité. Vos AWS charges de travail peuvent continuer à s'exécuter sur les mêmes comptes qu'AMS exploitait.

L'équipe qui fournira les services d'exploitation de votre infrastructure à l'avenir doit être incluse pour définir les personnes, les outils et les processus que vous utiliserez après votre déconnexion avec Accelerate. AMS abandonne certains outils, tels que les glissières de sécurité et les journaux, pour permettre le développement d'un environnement et d'un modèle d'exploitation « futurs ». Consultez attentivement la documentation suivante pour comprendre les outils que vous pouvez continuer à utiliser et comment demander à déconnecter un compte.

Effets d'offboarding AMS Accelerate

Lorsque vous vous préparez à quitter Accelerate, gardez à l'esprit les points suivants.

- Accès : La `ams-access-management` AWS CloudFormation pile qui définit le `ams-access-management` AWS Identity and Access Management rôle n'est pas supprimée. Après le déchargement, ces ressources restent, mais ne sont pas utilisées par les autres composants laissés pour compte. Vous pouvez supprimer la pile et le rôle à votre convenance.
- Rétention des ressources AMS : après le déchargement, certaines ressources AMS restent dans votre compte. Pour savoir quelles ressources sont conservées et ce que vous pouvez en faire, consultez la `resource_inventory.zip`feuille de calcul (compressée).
- Automatisation : après le déchargement, les runbooks d'automatisation AWS SSM sélectionnés par AMS et les fonctions AWS Lambda ne sont plus disponibles.
- Gestion des sauvegardes : AMS utilise la gestion des sauvegardes pour prendre des instantanés de vos ressources. Après le désenclavement, vous pouvez continuer à utiliser les plannings, la fréquence et les périodes de rétention de sauvegarde définis sur, à l' AWS Backup exception des plans de sauvegarde AMS ; voirSélectionnez un plan de sauvegarde AMS. Les AWS Identity and Access Management ressources créées par AMS Backup Orchestrator sont supprimées, mais pas les coffres-forts de sauvegarde créés par AMS et la clé correspondante. AWS KMS Accelerate ne surveille plus les tâches de sauvegarde ni n'effectue d'actions de restauration en cas d'incident.
- Optimisation des coûts : après le déchargement, le planificateur de ressources AMS est supprimé. AMS Resource Scheduler vous aide à réduire les coûts opérationnels en arrêtant les ressources qui ne sont pas utilisées et en les redémarrant lorsque leur capacité est nécessaire. AMS ne continue pas à fournir des recommandations d'optimisation des coûts. Pour plus de détails sur le planificateur de ressources, voir Optimisation des coûts avec AMS Resource Scheduler.
- Experts désignés : après le désenclavement, votre responsable de prestation de services cloud (CSDM) désigné et un architecte cloud (CA) ne fournissent plus de conseils, ne fournissent plus

de rapports ou ne favorisent plus l'excellence opérationnelle et de sécurité pour vos comptes Accelerate externes.

- Gestion des incidents : La gestion des incidents est le processus utilisé par le service AMS pour répondre aux incidents que vous avez signalés. Après le désenclavement, Accelerate ne détecte plus les incidents et n'y répond plus, et n'aide plus votre équipe à résoudre les problèmes. Vous ne pourrez pas échanger de communications relatives à des incidents ou à des demandes de service avec Accelerate et l'accès à la console Accelerate pour vos comptes Accelerate est désactivé.
- Journalisation et création de rapports : après le déchargement, vous conservez les journaux stockés à la suite de CloudWatch CloudTrail, et les journaux de flux VPC. Vous pouvez laisser la configuration de ces services telle quelle pour continuer à générer des journaux ; toutefois, AMS ne surveille plus ces configurations. Accelerate ne fournit plus le rapport de service mensuel qui résume les indicateurs de performance clés d'AMS. Vous conservez les données générées par le Self-Service Reporting (SSR) (voirRapports en libre-service), mais Accelerate n'en génère pas de nouvelles.
- Surveillance : La surveillance est le processus utilisé par le service AMS pour suivre vos ressources. Lors du décollage, AMS supprime les outils spécifiques à AMS, tels que Alarm Manager et Resource Tagger, ainsi que toutes les règles d' EventBridge événements et les CloudWatch alarmes déployées par AMS dans le cadre de la ligne de base de surveillance AMS. Accelerate ne répondra plus aux alarmes ni n'en configurera de nouvelles après le débarquement. Pour plus de détails sur Alarm Manager et Resource Tagger, voir Gestionnaire d'alarmes basé sur des balises et Resource Tagger.
- Outils opérationnels : AMS Accelerate peut fournir des opérations continues pour l'infrastructure de votre charge de travail dans AWS. Après avoir déconnecté un compte Accelerate, vous n'avez plus accès à des outils tels que Resource Tagger pour vous aider à étiqueter vos ressources en fonction de règles, ou à la configuration automatique des instances pour installer les agents requis dans vos EC2 instances. CloudWatch et les agents SSM sur les instances restent en place avec les configurations existantes. Le profil `AMSOSConfigurationCustomerInstanceRole` IAM et le `AMSInstanceProfileBasePolicy` sont détachés de vos instances et supprimés de vos comptes Accelerate.
- Gestion des correctifs : la gestion des correctifs est le processus utilisé par le service AMS pour mettre à jour vos EC2 instances. Après le déchargement, AMS ne crée plus de capture instantanée de l'instance avant l'application du correctif, n'installe plus et ne surveille plus l'installation du correctif, et ne vous informe plus du résultat. Vous conservez les lignes de base des correctifs et les instantanés créés dans le passé. De plus, la configuration de vos fenêtres de maintenance des correctifs est conservée, mais les correctifs ne sont plus installés par Accelerate.

- Gestion des problèmes : après le déchargement, Accelerate n'effectue plus d'analyse pour identifier et étudier les problèmes et pour en identifier la cause première.
- Sécurité : La gestion de la sécurité est le processus utilisé par le service AMS pour protéger vos ressources. Après le déchargement, vous conservez votre GuardDuty détecteur et vos résultats Amazon, ainsi que toutes AWS Config les règles que vous avez créées. AWS Config les règles déployées par Accelerate sont supprimées. Accelerate ne surveille plus, ne corrige plus ni ne rapporte les résultats de ces outils.
- Date de fin du service : La date de fin du service est le dernier jour du mois civil suivant la fin de la période de préavis de résiliation requise de 30 jours. Si la fin de la période de préavis de résiliation requise tombe après le 20e jour du mois civil, la date de fin du service est le dernier jour du mois civil suivant. Voici des exemples de scénarios relatifs aux dates de résiliation.
  - Si l'avis de résiliation est fourni le 12 avril, le préavis de 30 jours prend fin le 12 mai. La date de fin du service est le 31 mai.
  - Si un préavis de résiliation est fourni le 29 avril, le préavis de 30 jours prend fin le 29 mai. La date de fin du service est le 30 juin.

Déconnexion d'AMS Accelerate avec dépendance à Alarm Manager et Resource Tagger

AWS CloudFormation Les piles personnalisées qui déploient des configurations liées à Alarm Manager ou Resource Tagger, ainsi que les piles de configuration Alarm Manager et Resource Tagger fournies par AMS, restent dans votre compte lorsque vous quittez AWS Managed Services.

Pour supprimer les piles de configuration AMS pendant le processus de déchargement, vous devez supprimer toutes les dépendances et références sur Alarm Manager ou Resource Tagger des CloudFormation modèles personnalisés avant de lancer le processus de déchargement. La suppression des références permet de s'assurer que les piles sont correctement supprimées de votre compte lorsque vous quittez AMS.

> **Important**
>
> Passez en revue attentivement vos CloudFormation modèles et supprimez toute référence à Alarm Manager et Resource Tagger avant de commencer le processus de déconnexion. Dans le cas contraire, ces piles pourraient être conservées sur votre compte, même après votre départ d'AMS. Notez que bien que ces piles contiennent des informations de

configuration spécifiques à Alarm Manager et Resource Tagger, leur présence n'entraîne pas de frais ou de frais permanents.

Obtenir une assistance pour le désenclavement d'un compte Accelerate

AMS déconnecte votre compte après avoir reçu un préavis d'au moins 30 jours par le biais d'une demande de résiliation du service de compte AMS. La date de fin du service est le dernier jour du mois civil suivant la fin de la période de préavis de résiliation requise de 30 jours ; à condition que, si la fin de la période de préavis de résiliation requise tombe après le 20e jour du mois civil, la date de fin du service soit le dernier jour du mois civil suivant.

Pour demander la désinscription d'un compte, vous devez :

1. Soumettez une demande officielle de désinscription du compte à l'aide d'une demande de service. Une demande de service (SR) documentant tous les comptes que vous souhaitez déconnecter, ou une SR par compte.

   Dans la demande, fournissez la liste des comptes IDs à déconnecter, la raison du désembarquement et tout autre élément à prendre en compte.
2. Informez votre CSDM des comptes que vous souhaitez déconnecter et demandez-lui de l'aider à exécuter le processus de désinscription.

Paramètres de notification dans Accelerate

Les communications entre vous et AMS ont lieu pour de nombreuses raisons :

- Événements créés par les alertes de surveillance
- Notifications du service de correction, si vous avez activé le module complémentaire Patch
- Demandes de service et rapports d'incidents
- AWS Annonces importantes occasionnelles (votre CSDM vous contacte si une action de votre part est requise)

Toutes les notifications sont envoyées à l'aide d'un e-mail que vous avez fourni pour les notifications de correctif lors de votre intégration. Dans le cas contraire, les notifications sont envoyées à l'adresse e-mail par défaut que vous avez fournie à AMS lors de votre intégration. Comme il est difficile de tenir

à jour les e-mails individuels, nous vous recommandons d'utiliser un e-mail de groupe qui peut être mis à jour de votre côté. Toutes les notifications qui vous sont envoyées sont également reçues par les opérations AMS et analysées avant d'apporter une réponse.

Vous pouvez utiliser des listes de contacts nommées pour les notifications non basées sur les ressources, telles que les alertes basées sur GuardDuty ou AWS Config. Par exemple, vous pouvez avoir une liste nommée `SecurityContacts` et une autre nommée`OperationsContacts`. AMS envoie des alarmes et des notifications à ces listes.

Pour plus d’informations, consultez AWS Config Rapport de conformité des contrôles.

Marquage dans AMS Accelerate

La plupart des fonctionnalités d'Accelerate (application de correctifs, sauvegarde, surveillance) utilisent des balises et des profils de configuration pour décider quelles ressources gérer, quelles actions appliquer et quand les appliquer. Les tags sont des libellés que vous appliquez aux ressources. Les profils de configuration contiennent des règles basées sur ces balises.

Chaque fonctionnalité Accelerate a ses propres exigences en matière de balisage. Certaines fonctionnalités nécessitent l'utilisation de balises spécifiques, tandis que d'autres vous permettent d'utiliser les vôtres.

Pour plus d'informations sur les balises requises, consultezTags gérés par le client dans Accelerate.

Pour plus d'informations sur les tags qui peuvent être définis comme des clients, voir Tags fournis par le client dans Accelerate

Table des matières

- Balises dans AMS Accelerate
  - Qu'est-ce qu'une balise ?
  - Comment fonctionne le balisage
  - Tags gérés par le client dans Accelerate
    - Surveillance dans Accelerate
    - Configuration des balises pour les EC2 instances dans Accelerate
    - Gestion des balises pour les sauvegardes dans Accelerate
  - Accélérez la gestion des balises
  - Tags fournis par le client dans Accelerate
- Outils de gestion des balises pour Accelerate
  - Accélérez Resource Tagger
    - Qu'est-ce que Resource Tagger ?
    - Comment fonctionne Resource Tagger
    - Profils de configuration de Resource Tagger dans AMS Accelerate
      - Syntaxe et structure
    - Cas d'utilisation de Resource Tagger dans AMS Accelerate
      - Afficher les balises appliquées par Resource Tagger

        - Utilisation de Resource Tagger pour créer des balises
        - Empêcher le Resource Tagger de modifier les ressources
        - Exemple de profil de configuration
        - Fusion de la configuration par défaut
        - Désactivation de la configuration par défaut
        - Suppression des balises appliquées par Resource Tagger
        - Afficher ou modifier la configuration du Resource Tagger
        - Déploiement des modifications de configuration
        - Configuration de Terraform pour ignorer les balises Resource Tagger
        - Afficher le nombre de ressources gérées par Resource Tagger
    - Utilisation CloudFormation pour créer des balises pour AMS Accelerate
        - AWS CloudFormation Cas d'utilisation d'AMS Accelerate
            - Marquer une EC2 instance avec AWS CloudFormation for Accelerate
            - Marquer un AutoScaling groupe (ASG) avec AWS CloudFormation for Accelerate
            - Déploiement d'un profil de configuration avec AWS CloudFormation for Accelerate
    - Utiliser Terraform pour créer des balises pour AMS Accelerate

Balises dans AMS Accelerate

Table des matières

- Qu'est-ce qu'une balise ?
- Comment fonctionne le balisage
- Tags gérés par le client dans Accelerate
    - Surveillance dans Accelerate
    - Configuration des balises pour les EC2 instances dans Accelerate
    - Gestion des balises pour les sauvegardes dans Accelerate
- Accélérez la gestion des balises
- Tags fournis par le client dans Accelerate

Qu'est-ce qu'une balise ?

Une étiquette est une étiquette que vous attribuez à une AWS ressource. Chaque balise est constituée d'une clé et d'une valeur facultative que vous définissez toutes deux.

Vous utilisez des balises pour classer vos AWS ressources de différentes manières, par exemple par objectif, propriétaire ou environnement. Par exemple, vous pouvez définir un ensemble de balises pour les EC2 instances Amazon de votre compte, ce qui vous permet de suivre le propriétaire et le niveau de pile de chaque instance.

Les tags n'ont aucune signification sémantique pour Amazon EC2 et sont interprétés strictement comme des chaînes de caractères.

Pour en savoir plus, consultez la section AWS Ressources relatives au balisage.

Comment fonctionne le balisage

Il existe plusieurs manières d'appliquer des balises à vos ressources. Vous pouvez étiqueter les ressources directement dans la console de chaque AWS service lorsque vous créez la ressource, utiliser l'éditeur de AWS balises pour ajouter, supprimer ou modifier des balises pour plusieurs ressources, ou utiliser des outils de provisionnement tels que le tag de AWS CloudFormation ressource. AMS Accelerate fournit également le tagger de ressources AMS Accelerate que vous utilisez pour définir les règles d'un gestionnaire de cycle de vie des balises automatisé. Pour plus d'informations sur l'utilisation de Resource Tagger dans AMS Accelerate, consultezAccélérez Resource Tagger. AMS Accelerate fournit également des balises fournies par le client pour ajouter et supprimer des balises personnalisées à vos ressources AMS. Pour plus d'informations sur les balises fournies par le client, consultez. Tags fournis par le client dans Accelerate

Tags gérés par le client dans Accelerate

Certaines balises sont nécessaires pour déclencher diverses actions AMS Accelerate.

Table des matières

- Surveillance dans Accelerate
- Configuration des balises pour les EC2 instances dans Accelerate
- Gestion des balises pour les sauvegardes dans Accelerate

Surveillance dans Accelerate

AMS Accelerate surveille l'état, la disponibilité et la fiabilité des ressources prises en charge. Pour plus d'informations sur cette offre de service, consultezSurveillance et gestion des événements dans AMS Accelerate.

AMS Accelerate intègre régulièrement des dispositifs complémentaires Services AWS à la surveillance de base. Si vous utilisez la configuration par défaut du Resource Tagger, ces mises à jour sont automatiquement déployées sur vos comptes et les modifications sont répercutées sur les ressources prises en charge.

Pour accepter que vos EC2 instances Amazon soient gérées par AMS Accelerate, vous devez appliquer la balise suivante via le profil de personnalisation dans AppConfig ; pour plus d'informations, consultez Étape 3 : Création d'une configuration et d'un profil de configuration.

Appliquez la balise suivante à vos ressources :

Clé	Valeur
ams:rt:ams-managed	true

Par exemple, vous pouvez créer un document de configuration personnalisé comme celui-ci pour appliquer les balises à toutes vos ressources prises en charge par AMS EC2 :

```
{
    "AWS::EC2::Instance": {
        "AllEC2": {
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Important**
>
> N'oubliez pas de déployer vos modifications de configuration une fois que vous les avez apportées. Dans SSM AppConfig, vous devez déployer une nouvelle version de la configuration après l'avoir créée.

Les services autres qu'Amazon EC2 bénéficieront d'une surveillance de base par défaut. Pour refuser que vos ressources soient surveillées par AMS Accelerate, vous pouvez utiliser le profil de configuration de personnalisation pour exclure des ressources spécifiques ou Services AWS. Cela vous permet de contrôler les ressources qui doivent être dotées de balises de surveillance pour déployer les définitions d'alarme de base. Consultez Cas d'utilisation de Resource Tagger dans AMS Accelerate.

Utilisation de Resource Tagger

La configuration du tagger de ressources AMS Accelerate dans votre compte permet de garantir que les balises suivantes sont déployées automatiquement, si vous appliquez cette balise (ams:rt:ams-managed).

Les balises suivantes seront appliquées à vos ressources prises en charge à des fins de surveillance de base.

Clé	Valeur	Règle
ams : rt : ams-monitoring-policy	surveillée par AMS	S'applique à toutes les EC2 ressources prises en charge par AMS
ams : rt : ams-monitoring-policy-platform	ams-monitored-linux	S'applique à toutes les EC2 instances Amazon exécutant le système d'exploitation Linux
ams : rt : ams-monitoring-policy-platform	ams-monitored-windows	S'applique à toutes les EC2 instances Amazon exécutant le système d'exploitation Windows

Pour les autres services pris en charge

Appliquez les balises suivantes à vos ressources, conformément aux règles établies :

Clé	Valeur	Règle
ams : rt : ams-monitoring-policy	surveillée par AMS	S'applique à toutes les ressources prises en charge par la surveillance AMS Accelerate.
ams : rt : ams-monitoring-with-kms	ams-monitored-with-kms	OpenSearch Domaine avec KMS
ams : rt : ams-monitoring-with-master	ams-monitored-with-master	OpenSearch Domaine avec nœud principal dédié

Si vous n'utilisez pas Resource Tagger

Consultez Accélérez les tags sans Resource Tagger pour obtenir de l'aide sur l'application des balises de surveillance appropriées à l'aide de méthodes autres que l'utilisation d'AMS Resource Tagger.

Configuration des balises pour les EC2 instances dans Accelerate

AMS Accelerate gère les agents sur vos EC2 instances Amazon, tels que l'agent SSM et l' CloudWatch agent. Pour plus d'informations sur cette offre de service, voir Configuration d'instance automatisée dans AMS Accelerate

Pour accepter que vos EC2 instances Amazon soient gérées par AMS Accelerate, vous devez appliquer la balise suivante à vos EC2 instances Amazon :

Clé	Valeur
ams:rt:ams-managed	true

Gestion des balises pour les sauvegardes dans Accelerate

AMS Accelerate gère la sauvegarde des ressources prises en charge. Pour plus d'informations sur cette offre de service, consultezGestion de la continuité dans AMS Accelerate.

La gestion des sauvegardes AMS Accelerate utilise des balises pour identifier les ressources qui doivent être automatiquement sauvegardées (et fournit également des fonctionnalités de sauvegarde manuelle). Vous pouvez utiliser n'importe quelle combinaison clé:valeur de balise pour associer vos ressources à des plans de sauvegarde. Pour activer les sauvegardes automatisées à l'aide du ams-default-backup-plan AWS Backup plan, vous devez appliquer la balise suivante à vos ressources prises en charge :

Clé	Valeur
ams:rt:backup-orchestrator	true

> **Note**
>
> Lors de l'intégration, AMS Accelerate étiquette toutes les ressources avec ams:rt : backup-orchestrator-onboarding avec la valeur true pour les instantanés à court intervalle et à courte durée de conservation. Ceci est géré par le plan ams-onboarding-backup-plande sauvegarde. Pour plus d'informations sur les AWS Backup forfaits gérés par AMS Accelerate, consultez. Sélectionnez un plan de sauvegarde AMS

Accélérez la gestion des balises

Lors de l'intégration à AMS Accelerate, plusieurs AWS ressources sont déployées sur votre compte. Pour que vous puissiez les identifier, ces ressources sont étiquetées avec les balises suivantes :

Clé	Valeur
AMS : propriétaire de la ressource	AMS
bras : resourceOwnerService	Une description du service AMS Accelerat e proposant cette ressource provient, par

Clé	Valeur
	exemple, AMS Deployment, Backup, Controls, Monitoring, Patch, etc.
AppId	AMSInfrastructure
AppName	
Environnement	

> **Note**
>
> Ces balises sont appliquées à l'aide de balises AWS CloudFormation au niveau de la pile et reposent sur la AWS CloudFormation propagation des balises vers les ressources créées. Pour plus d'informations, consultez la section Resource tag.

Tags fournis par le client dans Accelerate

Que sont les tags fournis par le client ?

Les balises fournies par le client sont une fonctionnalité du service AMS Accelerate utilisée pour spécifier les règles régissant la manière dont les ressources AMS sont étiquetées dans votre compte. Grâce aux balises fournies par le client, vous pouvez ajouter des balises personnalisées définies par l'utilisateur aux ressources AMS déployées sur vos comptes. La fonctionnalité de balises fournies par le client est automatiquement ajoutée aux comptes demandés lorsque vous en faites la demande à votre responsable de prestation de services cloud (CSDM) à l'aide d'un service automatisé. Notez que vous ne pouvez pas remplacer les balises AMS. Les balises AMS commencent par « ams : ».

Vous pouvez définir vos propres balises (étiquettes) et spécifier les fonctionnalités de ces balises pour toutes vos ressources AMS Accelerate. Vous pouvez fournir ces balises avant d'intégrer AMS afin que les balises AMS et vos balises personnalisées soient appliquées pendant le processus d'intégration. Vous pouvez également fournir des tags après l'intégration.

Comment puis-je ajouter des tags fournis par le client ?

Pour demander l'ajout de ces balises à vos ressources, contactez votre CSDM. Ces balises seront appliquées aux ressources AMS de votre compte.

Quelle est la portée des tags ?

Cette fonctionnalité n'est actuellement disponible que pour les clients Accelerate et dans les régions AWS commerciales. Vous pouvez ajouter des tags à tous les comptes que vous possédez ou à une liste spécifique de comptes.

> **Note**
>
> Ces balises s'appliquent uniquement aux ressources AMS et n'affectent pas vos propres ressources.

Outils de gestion des balises pour Accelerate

Table des matières

- Accélérez Resource Tagger
- Utilisation CloudFormation pour créer des balises pour AMS Accelerate
- Utiliser Terraform pour créer des balises pour AMS Accelerate

Accélérez Resource Tagger

Avec Resource Tagger, vous pouvez définir des règles régissant la manière dont les AWS ressources sont étiquetées dans votre compte. Lors de l'intégration d'un compte, AMS Accelerate déploie votre politique de balisage pour garantir que les ressources de vos comptes gérés sont étiquetées.

Table des matières

- Qu'est-ce que Resource Tagger ?
- Comment fonctionne Resource Tagger
- Profils de configuration de Resource Tagger dans AMS Accelerate
  - Syntaxe et structure
- Cas d'utilisation de Resource Tagger dans AMS Accelerate
  - Afficher les balises appliquées par Resource Tagger
  - Utilisation de Resource Tagger pour créer des balises

- Empêcher le Resource Tagger de modifier les ressources
- Exemple de profil de configuration
- Fusion de la configuration par défaut
- Désactivation de la configuration par défaut
- Suppression des balises appliquées par Resource Tagger
- Afficher ou modifier la configuration du Resource Tagger
- Déploiement des modifications de configuration
- Configuration de Terraform pour ignorer les balises Resource Tagger
- Afficher le nombre de ressources gérées par Resource Tagger

Qu'est-ce que Resource Tagger ?

Resource Tagger est un service AMS Accelerate qui vous permet de définir des règles régissant la manière dont les AWS ressources sont étiquetées dans votre compte. Il vise à vous fournir une visibilité complète sur la manière dont vos balises sont appliquées à vos AWS ressources.

Resource Tagger crée, met à jour et supprime automatiquement les balises sur les AWS ressources prises en charge, en fonction des règles de balisage que vous spécifiez dans vos profils de configuration. Par exemple, vous pouvez spécifier une règle qui applique une balise à un ensemble d' EC2 instances Amazon, indiquant qu'elles doivent être gérées par AMS Accelerate, ce qui entraîne la surveillance ou la sauvegarde des instances. Vous pouvez utiliser de telles balises pour identifier le statut de conformité des AWS ressources en fonction de la politique définie dans vos profils AWS AppConfig de configuration. Pour de plus amples informations, veuillez consulter AWS AppConfig.

AMS Accelerate fournit une configuration de balisage géré par défaut afin que vous puissiez faire surveiller vos ressources par AMS Accelerate. Vous définissez les ressources qui doivent être gérées par AMS Accelerate, et les règles de balisage géré garantissent que les ressources dotées des balises appropriées sont surveillées par AMS Accelerate.

Avec Resource Tagger, si vous le souhaitez, vous pouvez remplacer ou désactiver les balises gérées par AMS Accelerate par défaut, fournir vos propres règles de balisage pour répondre à vos politiques et utiliser d'autres mécanismes, tels que Terraform, pour éviter la dérive. Vous pouvez définir les exceptions à l'échelle, en fonction de vos opérations. Par exemple, vous pouvez définir une politique visant à appliquer des balises à toutes les EC2 instances Amazon dotées de plateformes prises en charge (telles que Windows et Linux) et à exclure du balisage une instance IDs spécifique.

> **Important**
>
> Resource Tagger contrôle tous les tags de votre compte dotés du préfixe ams:rt :. Toutes les balises commençant par ce préfixe sont supprimées sauf si elles sont présentes dans les règles de configuration de Resource Tagger. En résumé, toute balise commençant par ams:rt : sur les ressources prises en charge est considérée comme appartenant à Resource Tagger. Si vous balisez manuellement quelque chose avec, par exemple, ams:rt :, cette balise sera automatiquement supprimée si elle n'est pas spécifiée dans l'un des profils de configuration du Resource Tagger.

Comment fonctionne Resource Tagger

Lorsque votre compte est intégré à AMS Accelerate, deux documents de configuration JSON sont déployés sur votre compte dans. AWS AppConfig Les deux documents, appelés profils de configuration, sont des AMSManagedbalises, appelées profil de configuration par défaut et CustomerManagedTagsprofil de configuration de personnalisation. Vous utilisez le profil de configuration personnalisé pour définir vos propres politiques et règles pour vos comptes, et celles-ci ne sont pas remplacées par AMS Accelerate.

Les deux profils se trouvent dans l'application AMSResourceTagger et dans l'AMSInfrastructureenvironnement. Toutes les balises appliquées par le baliseur de ressources ont le préfixe de clé ams:rt :.

Profil de configuration de personnalisation :

Le profil de configuration de personnalisation est initialement vide au moment de l'intégration du compte ; toutefois, toutes les règles placées dans le document de profil sont appliquées, en plus des règles du profil de configuration par défaut. Toute configuration du profil de configuration de personnalisation est entièrement gérée par vous et n'est pas remplacée par AMS Accelerate, sauf à votre demande.

Vous pouvez spécifier les règles de balisage personnalisées que vous souhaitez dans le profil de configuration personnalisé pour les AWS ressources prises en charge, et vous pouvez également spécifier des modifications à la configuration par défaut gérée par AMS Accelerate ici, voir. Cas d'utilisation de Resource Tagger dans AMS Accelerate

> **Important**
>
> Si vous mettez à jour ce profil, le Resource Tagger applique automatiquement les modifications à toutes les ressources pertinentes de votre. Compte AWS Les modifications sont appliquées automatiquement, mais leur prise en compte peut prendre jusqu'à 60 minutes.

Vous pouvez mettre à jour ce profil à l'aide des outils AWS Management Console AWS CLI/SDK ou par le biais de ceux-ci. Pour plus d'informations sur la mise à jour d'un profil de configuration personnalisé, consultez le guide de AWS AppConfig l'utilisateur : Qu'est-ce que c'est AWS AppConfig ?

Profil de configuration par défaut :

Le document de profil de configuration par défaut est interne à AMS Accelerate et contient les règles par défaut fournies par AMS Accelerate que vous ne pouvez ni modifier ni supprimer définitivement. Ce profil peut être mis à jour à tout moment par AMS Accelerate et mis à votre disposition pour examen ; toutes les modifications que vous y avez apportées sont automatiquement supprimées. Si vous souhaitez modifier ou désactiver l'une des règles de configuration par défaut, vous utilisez le profil de configuration de personnalisation, voirCas d'utilisation de Resource Tagger dans AMS Accelerate.

Profils de configuration de Resource Tagger dans AMS Accelerate

Les profils de configuration permettent de garantir que les balises sont appliquées uniformément aux ressources tout au long de leur durée de vie.

Syntaxe et structure

Un profil de configuration est un objet JSON dont la structure est la suivante :

```
{
   "Options": {
      "ReadOnly": false
   },
   "ResourceType": {
      "ConfigurationID": {
      "Enabled": true,
```

```
      "Filter": { ... },
      "Tags": [  ...  ]
      },
      "ConfigurationID": {
      ...
      }
   },
   "ResourceType": {
     ...
   }
}
```

Options : (facultatif) Spécifiez les options relatives à la façon dont vous souhaitez qu' ResourceTagger elles se comportent. L'omission du bloc revient à définir les valeurs par défaut de toutes les options. Voir ci-dessous les paramètres des options disponibles :

- ReadOnly: (facultatif, la valeur par défaut est false) : Spécifie le ReadOnly mode pour Resource Tagger. Définissez cette valeur ReadOnly sur true pour désactiver la création ou la suppression de balises par Resource Tagger sur les ressources AWS. Pour de plus amples informations, veuillez consulter Empêcher le Resource Tagger de modifier les ressources.

ResourceType: Cette clé doit être l'une des chaînes prises en charge suivantes et représente toutes les configurations liées au type de ressource indiqué :

- AWS::AutoScaling::AutoScalingGroupe
- AWS::DynamoDB::Table
- AWS::EC2::Instance
- AWS::EC2::NatGateway
- AWS : EC2 : : VPNConnection
- AWS::EFS::FileSystem
- AWS::EKS::Cluster
- AWS::ElasticLoadBalancing::LoadBalancer
- AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS::Elasticsearch::Domain
- AWS::FSx::FileSystem
- AWS::OpenSearch::Domain

- AWS : :RDS : : DBCluster
- AWS : :RDS : : DBInstance
- AWS::Redshift::Cluster
- AWS::S3::Bucket
- AWS::Synthetics::Canary

ConfigurationID : cette clé doit être unique dans le document de profil et nommer de manière unique le bloc de configuration suivant. Si deux blocs de configuration d'un même ResourceTypebloc ont le même identifiant de configuration, celui qui apparaît en dernier dans le profil prend effet. Si vous spécifiez dans votre profil de personnalisation un ID de configuration identique à celui spécifié dans le document par défaut, le bloc de configuration défini dans le profil de personnalisation prend effet.

> **Important**
>
> Le ConfigurationID doit ***not***chevaucher le profil AMS Accelerate ; par exemple, il ne doit pas être AMSMonitoringLinux ou AMSMonitoringWindows, sinon il désactive la configuration correspondante du profil de configuration AMSManagedTags.

Activé (facultatif, la valeur par défaut est true) : indique si le bloc de configuration prend effet. Définissez ce paramètre sur false pour désactiver un bloc de configuration. Un bloc de configuration désactivé n'a aucun effet.

Filtre : Spécifie les ressources auxquelles s'applique la configuration. Chaque objet de filtre peut comporter l'un des champs suivants (mais un seul) :

- AWS::AutoScaling::AutoScalingGroupe :
  - AutoScalingGroupName: nom du groupe Autoscaling. Ce champ prend en charge la correspondance par caractères génériques.
- AWS::DynamoDB::Table:
  - TableName: nom de la table DynamoDB. Ce champ prend en charge la correspondance par caractères génériques.
- AWS::EC2::Instance:
  - AvailabilityZone: le filtre correspond à une EC2 instance dans la zone de disponibilité spécifiée. Ce champ prend en charge la correspondance par caractères génériques, donc *a correspond à us-east-1a, ap-northeast-1a, etc.

  - InstanceId: le filtre fait correspondre une EC2 instance à l'ID d'instance spécifié. Ce champ prend en charge la correspondance par caractères génériques. Ainsi, i-00000* correspondrait à toute instance dont l'ID d'instance commence par i-00000.
  - Plateforme : le filtre fait correspondre une EC2 instance à la plate-forme spécifiée. Les valeurs valides sont Windows, Linux ou le caractère générique * (pour correspondre à n'importe quelle plateforme).
- AWS::EC2::NatGateway:
  - NatGatewayId: ID de la passerelle NAT. Ce champ prend en charge la correspondance par caractères génériques.
  - État : état de la passerelle NAT (en attente | échec | disponible | suppression | supprimé ou caractère générique « * »)
  - VpcId: ID du VPC dans lequel réside la passerelle NAT. Ce champ prend en charge la correspondance par caractères génériques.
  - SubnetId: ID du sous-réseau dans lequel réside la passerelle NAT. Ce champ prend en charge la correspondance par caractères génériques
- AWS : EC2 : : VPNConnection :
  - VpnConnectionId: ID de la connexion. Ce champ prend en charge la correspondance par caractères génériques.
- AWS::EFS::FileSystem:
  - FileSystemId: ID du système de fichiers EFS. Ce champ prend en charge la correspondance par caractères génériques.
- AWS::EKS::Cluster:
  - ClusterName: nom du cluster. Ce champ prend en charge la correspondance par caractères génériques.
- AWS::ElasticLoadBalancing::LoadBalancer (Classic Load Balancer) :
  - LoadBalancerName: Le LoadBalancer nom. Ce champ prend en charge la correspondance par caractères génériques.
  - Schéma : Il peut être « connecté à Internet », « interne » ou « * » générique.
  - VPCId: le champ VPCId dans lequel l'équilibreur de charge est déployé peut être un caractère générique « * ».
- AWS::ElasticLoadBalancingV2::LoadBalancer (Application Load Balancer (ALB)) :
  - LoadBalancerArn: le nom de la ressource LoadBalancer Amazon (ARN).

  - DNSName: Le DNSName de LoadBalancer. Ce champ prend en charge la correspondance par caractères génériques.
  - LoadBalancerName: Le LoadBalancer nom. Ce champ prend en charge la correspondance par caractères génériques.
- AWS::Elasticsearch::Domain:
  - DomainId: celui DomainId de la ElasticSearch ressource. Ce champ prend en charge la correspondance par caractères génériques.
  - DomainName: celui DomainName de la ElasticSearch ressource. Ce champ prend en charge la correspondance par caractères génériques.
  - HasMasterNode: valeur booléenne vraie ou fausse. Correspond si le domaine possède un nœud maître dédié.
  - HasKmsKeyValeur booléenne vraie ou fausse. Correspond si le domaine possède une clé KMS pour le chiffrement au repos.
- AWS::FSx::FileSystem:
  - FileSystemId: ID du système de FSx fichiers. Ce champ prend en charge la correspondance par caractères génériques.
- AWS::OpenSearch::Domain:
  - DomainId: celui DomainId de la OpenSearch ressource. Ce champ prend en charge la correspondance par caractères génériques.
  - DomainName: celui DomainName de la OpenSearch ressource. Ce champ prend en charge la correspondance par caractères génériques.
  - HasMasterNode: booléen ; si le domaine possède un nœud maître dédié, cela peut être défini sur true.
  - HasKmsKey: si le domaine possède une clé KMS pour le chiffrement au repos, cela peut être défini sur true.
- AWS : :RDS : : : DBCluster
  - DBClusterIdentifiant : le filtre fait correspondre un identifiant de cluster RDS à l'identifiant spécifié. Ce champ ne prend pas en charge la correspondance par caractères génériques, un identifiant de cluster doit donc être spécifié.
  - Moteur : moteur utilisé par l'instance RDS. Ce champ prend en charge la correspondance par caractères génériques.
  - EngineVersion: La version du moteur. Ce champ prend en charge la correspondance par caractères génériques.

- AWS : :RDS : : : DBInstance
  - DBInstanceIdentifiant : le filtre fait correspondre une instance RDS à l'ID d'instance spécifié. Ce champ ne prend pas en charge la correspondance par caractères génériques, un identifiant d'instance doit donc être spécifié.
  - Moteur : moteur utilisé par l'instance RDS. Ce champ prend en charge la correspondance par caractères génériques.
  - EngineVersion: La version du moteur. Ce champ prend en charge la correspondance par caractères génériques.
- AWS::Redshift::Cluster:
  - ClusterIdentifier: L'identifiant du cluster. Ce champ prend en charge la correspondance par caractères génériques.
- AWS::S3::Bucket:
  - BucketName: nom du compartiment S3. Ce champ prend en charge la correspondance par caractères génériques.
- AWS::Synthetics::Canary:
  - CanaryName: Le nom du canari Synthetics.

Autres propriétés du filtre :

- Tag : Le filtre s'applique à toutes les ressources auxquelles le tag donné est déjà appliqué. La valeur de cette propriété doit être un objet JSON avec les champs suivants :
  - Clé : doit être une chaîne exacte et indique que les ressources doivent avoir une balise avec cette clé exacte.
  - Valeur : Spécifie la valeur correspondante pour la balise. Supporte les caractères génériques, de sorte qu'une valeur de Sample correspond à toute valeur se terminant par la chaîne Sample.
- Fn : :AND : tableau JSON d'objets JSON. Chaque objet suit les mêmes règles que le bloc de configuration du filtre. Cela indique que le filtre correspond à toute ressource correspondant à tous les sous-filtres.
- Fn : :OR : tableau JSON d'objets JSON. Chaque objet suit les mêmes règles que le bloc de configuration du filtre. Cela indique que le filtre correspond à toute ressource correspondant à l'un des sous-filtres.
- Fn : :NOT : un objet JSON qui suit les mêmes règles que le bloc de configuration du filtre. Cela indique que le filtre ne correspond explicitement à aucune ressource correspondant au sous-filtre. Utilisez-le pour spécifier les exclusions de vos règles de balisage.

Balises : balises à appliquer aux ressources correspondantes. (Voir Dénomination des balises et conventions d'utilisation.) Ce champ est un tableau de paires clé-valeur :

- Clé : clé de la balise à appliquer.
- Valeur : valeur de la balise à appliquer.

> **Note**
>
> Les balises appliquées par Resource Tagger ont toujours des clés qui commencent par ams:rt :. Si vous ne spécifiez pas ce préfixe dans votre profil, Resource Tagger l'insère pour vous. C'est ainsi que Resource Tagger distingue les balises qu'elle possède et gère des balises utilisées par d'autres outils à d'autres fins.

Cas d'utilisation de Resource Tagger dans AMS Accelerate

Cette section répertorie les actions fréquemment effectuées avec Resource Tagger.

Afficher les balises appliquées par Resource Tagger

Toutes les balises appliquées par Resource Tagger ont le préfixe de clé ams:rt :. Par exemple, la définition de balise suivante génère une balise avec la clé AMS:RT:SampleKey et la valeur SampleValue. Toutes les balises portant ce préfixe sont considérées comme faisant partie de Resource Tagger.

```
{
 "Key": "sampleKey",
 "Value": "sampleValue"
}
```

> **Important**
>
> Si vous créez manuellement votre propre tag avec le préfixe ams:rt :, il est considéré comme géré par Resource Tagger. Cela signifie que si la ressource est gérée par Resource Tagger, mais que les profils de configuration n'indiquent pas que la balise doit être appliquée, Resource Tagger supprime votre balise ajoutée manuellement. Si vous balisez manuellement des ressources gérées par Resource Tagger, n'utilisez pas le préfixe ams:rt : pour les clés de balise.

Utilisation de Resource Tagger pour créer des balises

Le tagger de ressources AMS Accelerate est un composant qui est déployé dans votre compte lors de l'intégration d'AMS Accelerate. Resource Tagger dispose d'un ensemble de règles configurables qui définissent la manière dont vos ressources doivent être étiquetées, puis il applique ces règles, en ajoutant et en supprimant automatiquement des balises sur les ressources pour garantir leur conformité à vos règles.

Si vous souhaitez utiliser le Resource Tagger pour étiqueter vos ressources, consultezAccélérez Resource Tagger.

Voici un exemple d'extrait de configuration de Resource Tagger qui ajoute la balise ams:rt:ams-managed avec la valeur true à toutes les instances Amazon. EC2 La balise ams:rt:ams-managed vous permet de faire surveiller vos ressources par AMS Accelerate.

```
{
    "AWS::EC2::Instance": {
        "SampleConfigurationBlock": {
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Warning**
>
> Soyez prudent lorsque vous spécifiez le nom de votre nouvelle configuration (`SampleConfigurationBlock`dans l'exemple fourni) car vous risquez de remplacer par inadvertance la configuration gérée par AMS par le même nom.

Empêcher le Resource Tagger de modifier les ressources

Le Resource Tagger peut être configuré sur un mode lecture seule qui l'empêche d'ajouter ou de supprimer des balises sur vos ressources. Cela est utile si vous souhaitez fournir votre propre mécanisme de balisage.

En mode lecture seule, Resource Tagger examine toujours les règles de balisage spécifiées dans les profils de configuration gérés et clients, et recherche les ressources qui ne respectent pas ces règles de balisage. Toutes les ressources non conformes sont signalées. AWS Config Celui AWS Config Rules que vous pouvez rechercher a le `AMSResourceTagger-` préfixe. Par exemple, la `AMSResourceTagger-EC2Instance` AWS Config règle évalue si des balises appropriées sont créées pour les `AWS::EC2::Instance` ressources en fonction du profil de configuration.

Resource Tagger s'arrête à ce stade et n'apporte aucune modification à vos ressources (il n'ajoute ni ne supprime de balises).

Vous pouvez activer le mode lecture seule en modifiant le profil de configuration client pour inclure la ReadOnlyclé dans le bloc Options. Par exemple, l'extrait de profil de configuration suivant montre à quoi cela pourrait ressembler :

```
{
    "Options": {
        "ReadOnly": true
    },
    "AWS::EC2::Instance": {
        [... the rest of your configuration ...]
    }
}
```

Resource Tagger réagira à cette nouvelle configuration dès la fin du déploiement et cessera d'ajouter et de supprimer des balises sur les ressources.

> **Note**
>
> Pour réactiver la modification des balises, remplacez la ReadOnlyvaleur par false ou supprimez complètement la clé, car la valeur par défaut est false.

Pour en savoir plus sur le paramètre OptionsSyntaxe et structure, reportez-vous à la section suivante.

Exemple de profil de configuration

L'exemple de document de profil suivant indique que toutes les EC2 instances Windows faisant partie d'une CloudFormation pile stack-* doivent être gérées par AMS Accelerate ; il exclut toutefois explicitement une EC2 instance particulière portant l'ID i-00000000000000001.

```
{
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "Windows"
                    },
                    {
                        "Tag": {
                            "Key": "aws:cloudformation:stack-name",
                            "Value": "stack-*"
                        }
                    },
                    {
                        "Fn::NOT": {
                            "InstanceId": "i-00000000000000001"
                        }
                    }
                ]
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Warning**
>
> Soyez prudent lorsque vous spécifiez le nom de votre nouvelle configuration (`SampleConfigurationBlock`dans l'exemple fourni) car vous risquez de remplacer par inadvertance la configuration gérée par AMS par le même nom.

Fusion de la configuration par défaut

Le profil de configuration par défaut est fourni par AMS Accelerate au moment de l'enregistrement du compte. Ce profil fournit des règles par défaut qui sont déployées dans votre compte.

Bien que vous ne puissiez pas modifier le profil de configuration par défaut, vous pouvez remplacer les paramètres par défaut en spécifiant un bloc de configuration dans votre profil de configuration personnalisé avec le même identifiant de configuration que le bloc de configuration par défaut. Dans ce cas, votre bloc de configuration remplace le bloc de configuration par défaut.

Par exemple, considérez le document de configuration par défaut suivant :

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
 }
}
```

Pour modifier la valeur de balise appliquée ici de `SampleValueA` à `SampleValueB` et appliquer la balise à toutes les instances, et pas uniquement aux instances Windows, vous devez fournir le profil de configuration de personnalisation suivant :

```
{
 "AWS::EC2::Instance": {
```

```
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "*"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueB"
   }]
  }
 }
}
```

> **Important**
>
> N'oubliez pas de déployer vos modifications de configuration une fois que vous les avez apportées. Pour de plus amples informations, veuillez consulter Déploiement des modifications de configuration. Dans SSM AppConfig, vous devez déployer une nouvelle version de la configuration après l'avoir créée.

Désactivation de la configuration par défaut

Vous pouvez désactiver une règle de configuration par défaut en ajoutant un bloc de configuration avec le même identifiant de configuration à votre profil de configuration personnalisé et en attribuant au champ Enabled la valeur false.

Par exemple, si la configuration suivante était présente dans le profil de configuration par défaut :

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
 }
```

```
}
```

Vous pouvez désactiver cette règle de balisage en incluant les éléments suivants dans votre profil de configuration de personnalisation :

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": false
  }
 }
}
```

> **Important**
>
> N'oubliez pas de déployer vos modifications de configuration une fois que vous les avez apportées ; pour plus d'informations, consultezDéploiement des modifications de configuration. Dans SSM AppConfig, vous devez déployer une nouvelle version de la configuration après l'avoir créée.

Suppression des balises appliquées par Resource Tagger

Toutes les balises préfixées par ams:rt sont supprimées par Resource Tagger si elles n'existent pas dans les profils de configuration ou, si elles existent, si le filtre ne correspond pas. Cela signifie que vous pouvez supprimer les balises appliquées par Resource Tagger en effectuant l'une des opérations suivantes :

- Modification de la section de configuration de personnalisation qui définit le tag.
- Ajout d'une exception pour les ressources spécifiques afin qu'elles ne correspondent plus au filtre.

Par exemple : si une instance Linux possède les balises suivantes :

```
"Tags": [{
    "Key": "ams:rt:MyOwnTag",
    "Value": true
},{
    "Key": "myTag",
    "Value": true
```

```
}]
```

Et vous déployez le profil de configuration de Resource Tagger suivant :

```
{
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Platform": "Windows"
            },
            "Tags": [{
                "Key": "ams:rt:ams-managed",
                "Value": "true"
            }]
        }
    }
}
```

Resource Tagger réagit aux nouvelles modifications de configuration et la seule balise de l'instance devient :

```
"Tags": [{
    "Key": "myTag",
    "Value": true
}]
```

Warning

Soyez prudent lorsque vous spécifiez le nom de votre nouvelle configuration (`SampleConfigurationBlock`dans l'exemple fourni) car vous risquez de remplacer par inadvertance la configuration gérée par AMS par le même nom.

Important

N'oubliez pas de déployer vos modifications de configuration une fois que vous les avez apportées ; pour plus d'informations, consultezDéploiement des modifications de

configuration. Dans SSM AppConfig, vous devez déployer une nouvelle version de la configuration après l'avoir créée.

Afficher ou modifier la configuration du Resource Tagger

Les deux profils de configuration JSON, AMSManagedTags et CustomerManagedTags, déployés sur votre compte dans AWS AppConfig lors de l'intégration et du stockage dans l'application AMSResource Tagger, ainsi que dans l'AMSInfrastructureenvironnement, peuvent être consultés via AppConfig l'GetConfigurationAPI.

Voici un exemple de cet GetConfiguration appel :

```
aws appconfig get-configuration
 --application AMSResourceTagger
 --environment AMSInfrastructure
 --configuration AMSManagedTags
 --client-id ANY_STRING
 outfile.json
```

Application : unité AppConfig logique fournissant des fonctionnalités, pour le Resource Tagger, il s'agit de AMSResource Tagger.

- Environnement : AMSInfrastructure.
- Configuration : pour afficher les définitions de balises par défaut d'AMS Accelerate, la valeur est AMSManaged Tags, tandis que pour afficher les définitions des balises client, la valeur est CustomerManagedTags.
- ID client : identifiant unique de l'instance d'application, il peut s'agir de n'importe quelle chaîne.
- Les définitions des balises peuvent ensuite être consultées dans le fichier de sortie spécifié, dans ce cas, outfile.json.

Les définitions des alarmes peuvent ensuite être consultées dans le fichier de sortie spécifié, dans ce cas, outfile.json.

Vous pouvez voir quelle version de configuration est déployée sur votre compte en consultant les déploiements antérieurs dans l'AMSInfrastructureenvironnement.

Pour contourner les règles relatives aux balises, procédez comme suit :

Toutes les règles de balise existantes peuvent être remplacées en mettant à jour le profil de personnalisation avec AWS CloudFormation Déploiement d'un profil de configuration avec AWS CloudFormation for Accelerate ou directement à l'aide de l'API AppConfig d'CreateHostedConfigurationVersionutilisation. L'utilisation du même identifiant de configuration comme règle de balise de configuration par défaut remplace la règle par défaut et applique la règle personnalisée à sa place.

Pour déployer les modifications apportées au CustomerManagedTagsdocument :

Après avoir apporté des modifications au profil de configuration de personnalisation, vous devez déployer les modifications correspondantes. Pour déployer les nouvelles modifications, AppConfig l'StartDeploymentAPI doit être exécutée à l'aide de la AWS AppConfig console ou de la CLI.

Déploiement des modifications de configuration

Une fois la personnalisation terminée, ces modifications doivent être déployées via l' AWS AppConfig StartDeploymentAPI. Les instructions suivantes indiquent comment effectuer un déploiement à l'aide du AWS CLI. Vous pouvez également utiliser le AWS Management Console pour effectuer ces modifications. Pour plus d'informations, voir Étape 5 : Déploiement d'une configuration.

```
aws appconfig start-deployment
--application-id <application_id>
--environment-id <environment_id>
--deployment-strategy-id <deployment_strategy_id>
--configuration-profile-id <configuration_profile_id>
--configuration-version 1
```

- ID de l'application : ID de l'application AMSResource Tagger. Obtenez-le avec l'appel ListApplicationsd'API.
- ID d'environnement : ID d'environnement ; obtenez-le avec l'appel ListEnvironmentsd'API.
- ID de stratégie de déploiement : ID de stratégie de déploiement ; obtenez-le avec l'appel ListDeploymentStrategiesd'API.
- ID du profil de configuration : ID du profil de configuration de CustomerManagedTags ; obtenez-le avec l'appel ListConfigurationProfilesd'API.
- Version de configuration : version du profil de configuration que vous souhaitez déployer.

> **Important**
>
> Resource Tagger applique les balises comme indiqué dans les profils de configuration. Toutes les modifications manuelles que vous apportez (avec le AWS Management Console CloudWatch CLI/SDK) aux balises de ressources sont automatiquement annulées. Assurez-vous donc que vos modifications sont définies via Resource Tagger. Pour savoir quelles balises sont créées par le Resource Tagger, recherchez les clés de balise préfixées par. `ams:rt:`

Limitez l'accès au déploiement StartDeploymentet aux actions de l'StopDeploymentAPI aux utilisateurs de confiance qui comprennent les responsabilités et les conséquences du déploiement d'une nouvelle configuration sur vos cibles.

Pour en savoir plus sur l'utilisation AWS AppConfig des fonctionnalités pour créer et déployer une configuration, consultez la documentation sur Travailler avec AWS AppConfig.

Configuration de Terraform pour ignorer les balises Resource Tagger

Si vous utilisez Terraform pour approvisionner vos ressources et que vous souhaitez utiliser Resource Tagger pour étiqueter vos ressources, les balises Resource Tagger peuvent être identifiées comme dérivées par Terraform.

Vous pouvez configurer Terraform pour ignorer toutes les balises Resource Tagger à l'aide du bloc de configuration du cycle de vie ou du bloc de configuration global ignore_tags. Pour plus d'informations, consultez la documentation Terraform sur le balisage des ressources lors du balisage des ressources.

L'exemple suivant montre comment créer une configuration globale pour ignorer toutes les balises commençant par le préfixe `ams:rt:` de balise Resource Tagger :

```
provider "aws" {
  # ... potentially other configuration ...

  ignore_tags {
    key_prefixes = ["ams:rt:"]
  }
}
```

Afficher le nombre de ressources gérées par Resource Tagger

Resource Tagger envoie des métriques toutes les heures à Amazon CloudWatch, dans l'espace de `AMS/ResourceTagger` noms. Les métriques sont émises uniquement pour les types de ressources pris en charge par Resource Tagger.

Nom de la métrique	Dimensions	Description
ResourceCount	Composant, ResourceType	Nombre de ressources (du type de ressource spécifié) déployées dans cette région. Unités : nombre
ResourcesMissingManagedTags	Composant, ResourceType	Nombre de ressources (du type de ressource spécifié) qui nécessitent des balises gérées, selon les profils de configuration, mais qui n'ont pas encore été étiquetées par Resource Tagger. Unités : nombre
UnmanagedResources	Composant, ResourceType	Nombre de ressources (du type de ressource spécifié) auxquelles aucune balise gérée n'est appliquée par Resource Tagger. Généralement, ces ressources ne correspondent à aucun bloc de configuration Resource Tagger ou sont explicitement exclues des blocs de configuration. Unités : nombre
MatchingResourceCount	Composant ResourceType, ConfigClauseName	Nombre de ressources (du type de ressource spécifié) correspondant au bloc de configuration Resource Tagger. Pour qu'une ressource corresponde au bloc de configuration, le bloc doit être activé et la ressource doit correspondre au filtre du bloc. Unités : nombre

Ces statistiques sont également consultables sous forme de graphiques, dans le tableau de bord AMS-Resource-Tagger-Reporting-Dashboard. Pour voir le tableau de bord, depuis la console de CloudWatch gestion Amazon, sélectionnez AMS-Resource-Tagger-Reporting-Dashboard. Par défaut, les graphiques de ce tableau de bord affichent les données de la période de 12 heures précédente.

AMS Accelerate déploie des CloudWatch alarmes sur votre compte pour détecter les augmentations significatives du nombre de ressources non gérées, par exemple les ressources exclues de la gestion par AMS Resource Tagger. AMS Operations étudiera les augmentations des ressources non gérées qui dépassent : soit trois ressources du même type, soit une augmentation de 50 % par rapport à toutes les ressources du même type. Si le changement ne semble pas être délibéré, AMS Operations peut vous contacter pour examiner le changement.

Utilisation CloudFormation pour créer des balises pour AMS Accelerate

Vous pouvez les utiliser AWS CloudFormation pour appliquer des balises au niveau de la pile (voir AWS CloudFormation la documentation, balise de ressource) ou au niveau des ressources individuelles (par exemple, voir Marquage de vos EC2 ressources Amazon).

> **Important**
>
> Certains composants du service AMS Accelerate nécessitent des balises avec le préfixe ams:rt :. Resource Tagger pense être propriétaire de ces balises et les supprimera si aucune règle de configuration de Resource Tagger ne les autorise. Vous devez toujours déployer un profil de configuration Resource Tagger pour ces balises, même si vous utilisez AWS CloudFormation Terraform.

AWS CloudFormation Cas d'utilisation d'AMS Accelerate

Cette section répertorie les actions fréquemment effectuées avec AWS CloudFormation.

Rubriques

- Marquer une EC2 instance avec AWS CloudFormation for Accelerate
- Marquer un AutoScaling groupe (ASG) avec AWS CloudFormation for Accelerate
- Déploiement d'un profil de configuration avec AWS CloudFormation for Accelerate

Marquer une EC2 instance avec AWS CloudFormation for Accelerate

Voici un exemple de la façon dont vous pouvez appliquer la balise ams:rt:ams-managed avec la valeur true à une instance Amazon gérée par. EC2 AWS CloudFormation La balise ams:rt:ams-managed vous permet de faire surveiller vos ressources par AMS Accelerate.

```
 Type: AWS::EC2::Instance

Properties:
  InstanceType: "t3.micro"

  # ...other properties...

  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

Marquer un AutoScaling groupe (ASG) avec AWS CloudFormation for Accelerate

Voici un exemple de la façon dont vous pouvez appliquer la balise ams:rt:ams-managed avec la valeur true à un groupe Auto Scaling géré par. AWS CloudFormation Notez que le groupe Auto Scaling propagera ses balises aux EC2 instances Amazon qu'il a créées. La balise ams:rt:ams-managed vous permet de faire surveiller vos ressources par AMS Accelerate.

```
  Type: AWS::AutoScaling::AutoScalingGroup
Properties:
  AutoScalingGroupName: "SampleASG"

  # ...other properties...

  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

Déploiement d'un profil de configuration avec AWS CloudFormation for Accelerate

Si vous souhaitez déployer votre profil de `CustomerManagedTags` configuration à l'aide des modèles suivants AWS CloudFormation, vous pouvez utiliser les CloudFormation modèles suivants. Entrez la configuration JSON souhaitée dans le `AMSResourceTaggerConfigurationVersion.Content` champ.

Lorsque vous déployez les modèles dans une CloudFormation pile ou un ensemble de piles, le déploiement de la `AMSResourceTaggerDeployment` ressource échoue si vous n'avez pas suivi le format JSON requis pour la configuration. Voir Syntaxe et structure pour plus de détails sur le format attendu.

Pour obtenir de l'aide sur le déploiement de ces modèles sous forme de CloudFormation pile ou d'ensemble de piles, consultez la AWS CloudFormation documentation correspondante ci-dessous :

- Création d'une pile sur la AWS CloudFormation console
- Création d'une pile avec AWS CLI
- Création d'un ensemble de piles

> **Note**
>
> Si vous déployez une version de configuration à l'aide de l'un de ces modèles, puis que vous supprimez ensuite l'ensemble CloudFormation de piles ou de piles, la version de configuration du modèle restera la version actuellement déployée et aucun déploiement supplémentaire ne sera effectué. Si vous souhaitez revenir à une configuration par défaut, vous devez soit déployer manuellement une configuration vide (c'est-à-dire simplement`{}`), soit mettre à jour votre pile avec une configuration vide, plutôt que de supprimer la pile.

JSON

```
{
  "Description": "Custom configuration for the AMS Resource Tagger.",
  "Resources": {
    "AMSResourceTaggerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "Content": "{\"Options\": {\"ReadOnly\": false}}",
        "ContentType": "application/json"
```

```
      }
    },
    "AMSResourceTaggerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSResourceTaggerConfigurationVersion"
        },
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Resource Tagger.
Resources:
  AMSResourceTaggerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      Content: |
        {
          "Options": {
            "ReadOnly": false
          }
        }
```

```
      ContentType: application/json
  AMSResourceTaggerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      ConfigurationVersion:
        !Ref AMSResourceTaggerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-ResourceTagger-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-ResourceTagger-Configuration-EnvironmentId
```

Utiliser Terraform pour créer des balises pour AMS Accelerate

Si vous ne souhaitez pas utiliser AMS Accelerate Resource Tagger, vous pouvez appliquer vos propres balises à l'aide de Terraform. Toutefois, si vous ne souhaitez pas utiliser le Resource Tagger en raison de sa dérive par rapport à vos définitions Terraform, il existe un moyen d'utiliser le Resource Tagger et d'ignorer la dérive qu'il provoque ; voir. Configuration de Terraform pour ignorer les balises Resource Tagger

> **Important**
>
> Certains composants du service AMS Accelerate nécessitent des balises avec le préfixe ams:rt :. Resource Tagger pense être propriétaire de ces balises et les supprime si aucune règle de configuration de Resource Tagger ne les autorise. Vous devez déployer un profil de configuration Resource Tagger pour ces balises, même si vous utilisez AWS CloudFormation Terraform.

Voici un exemple de la manière dont vous pouvez appliquer la balise ams:rt:ams-managed avec la valeur true à une instance Amazon gérée par Terraform. EC2 La balise ams:rt:ams-managed vous permet de faire surveiller vos ressources par AMS Accelerate.

```
resource "aws_instance" "sample_linux_instance" {
  # ...ami and other properties...
```

```
    instance_type = "t3.micro"

    tags = {
        "ams:rt:ams-managed" = "true"
    }
}
```

Voici un exemple de la façon dont vous pouvez appliquer la balise ams:rt:ams-managed avec la valeur true à un groupe Auto Scaling géré par Terraform. Notez que le groupe Auto Scaling propage ses balises aux EC2 instances Amazon qu'il a créées. La balise ams:rt:ams-managed vous permet de faire surveiller vos ressources par AMS Accelerate.

```
  resource "aws_autoscaling_group" "sample_asg" {
    # ...other properties...

    name = "terraform-sample"

    tags = {
        "ams:rt:ams-managed" = "true"
    }
}
```

Pour une description de la gestion des balises de ressources créées par Terraform, consultez. [Configuration de Terraform pour ignorer les balises Resource Tagger]

Rapports d'incidents, demandes de service et questions de facturation dans AMS Accelerate

Avec AMS Accelerate, vous pouvez demander de l'aide pour des problèmes opérationnels et des demandes à tout moment via le Centre de AWS support du AWS Management Console. Les ingénieurs opérationnels d'AMS Accelerate sont disponibles pour répondre à vos incidents et à vos demandes de service round-the-clock, avec des accords de niveau de service (SLAs) relatifs au temps de réponse pour le service. Les ingénieurs des opérations d'AMS Accelerate vous informent de manière proactive des alertes et des questions importantes en utilisant les mêmes mécanismes.

AMS Accelerate fournit une gamme de services opérationnels pour vous aider à atteindre l'excellence opérationnelle sur AWS. Pour comprendre rapidement comment AMS aide vos équipes à atteindre l'excellence opérationnelle globale AWS Cloud grâce à certaines de nos principales capacités opérationnelles, notamment le service d' round-the-clockassistance, la surveillance proactive, la sécurité, l'application de correctifs, la journalisation et la sauvegarde, consultez les diagrammes d'architecture de référence AMS.

Rubriques

- Gestion des incidents dans AMS Accelerate
- Gestion des demandes de service dans Accelerate
- Test des rapports d'incidents et des demandes de service dans Accelerate
- Questions relatives à la facturation pour AMS Accelerate

Gestion des incidents dans AMS Accelerate

Dans AMS Accelerate, vous utilisez le AWS Support Center Consolepour déposer des rapports d'incidents. Les incidents sont des problèmes de Service AWS performance qui ont un impact sur votre environnement géré, tel que déterminé par AMS Accelerate ou par vous-même. Les incidents identifiés par l'équipe AMS Accelerate sont d'abord reçus sous forme d'événements (modification de l'état du système capturée par le monitoring). Si un seuil configuré est dépassé, l'événement déclenche une alarme, également appelée alerte. L'équipe opérationnelle d'AMS Accelerate détermine si l'événement n'a pas d'impact, s'il s'agit d'un incident (interruption ou dégradation du service) ou d'un problème (cause première sous-jacente d'un ou de plusieurs incidents).

> **Note**
>
> L'équipe AMS Accelerate reçoit également les incidents que vous avez créés par programmation à l'aide de l'API AWS Support avec le code de service. `service-ams-operations-report-incident`

Pour plus d'informations sur l'utilisation Support, consultez Getting started with Support.

Qu'est-ce que la gestion des incidents ?

La gestion des incidents est le processus utilisé par AMS pour enregistrer, agir, communiquer la progression et notifier les incidents actifs.

L'objectif du processus de gestion des incidents est de garantir que le fonctionnement normal de votre service géré est rétabli le plus rapidement possible, que l'impact commercial est minimisé et que toutes les parties concernées sont tenues informées.

Les exemples d'incidents incluent (sans toutefois s'y limiter) la perte ou la dégradation de la connectivité réseau, un processus ou une API qui ne répondent pas, ou une tâche planifiée qui n'est pas exécutée (par exemple, une sauvegarde échouée).

Le graphique suivant illustre le flux de travail d'un incident que vous avez signalé à AMS.

Ce graphique illustre le flux de travail d'un incident qui vous a été signalé par AMS.

Priorité de l'incident

Les incidents créés dans le centre de support AWS, la console ou l'API de support (SAPI) ont des classifications différentes de celles des incidents créés dans la console AMS.

- Faible : les fonctions non critiques de votre service ou de votre application métier liées aux ressources AWS ou AMS sont affectées.
- Moyen : un service ou une application métier lié aux ressources AWS and/or AMS est modérément impacté et fonctionne de manière dégradée.
- Élevé : votre activité est fortement impactée. Les fonctions critiques de votre application liées aux ressources AWS and/or AMS ne sont pas disponibles. Réservé aux pannes les plus critiques affectant les systèmes de production.

> **Note**
>
> La console de support AWS propose cinq niveaux de priorité des incidents que nous traduisons en trois niveaux AMS.

Comment fonctionnent la réponse et la résolution des incidents

AMS Accelerate utilise les meilleures pratiques de gestion des incidents de gestion des services informatiques (ITSM) pour rétablir le service, en cas de besoin, le plus rapidement possible.

Nous fournissons une follow-the-sun assistance 24 heures sur 24, 7 jours sur 7 et 365 jours par an par le biais de centres d'opérations du monde entier, avec des opérateurs dédiés qui surveillent activement les tableaux de bord de surveillance et les files d'attente d'incidents.

Nos ingénieurs d'exploitation utilisent des outils internes de suivi des incidents pour identifier, enregistrer, classer, classer par ordre de priorité, diagnostiquer, résoudre et clôturer les incidents ; nous vous fournissons des mises à jour sur toutes ces activités par le biais du Centre de AWS support et de l'API de AWS support. Nos opérateurs s'appuient sur une variété d'outils de AWS support internes pour les aider dans toutes ces activités. Ces opérateurs connaissent parfaitement l'infrastructure soutenue par AMS Accelerate et possèdent des compétences techniques de niveau expert pour résoudre les problèmes de support identifiés. Si nos opérateurs ont besoin d'assistance, les équipes de support et AWS de service Premium sont disponibles.

Une fois votre incident reçu par l'équipe opérationnelle d'AMS Accelerate, nous validons la priorité et la classification en travaillant avec vous si des clarifications sont nécessaires. Par exemple, s'il vaut mieux classer le rapport d'incident en tant que demande de service, il est reclassé et l'équipe chargée des demandes de service AMS Accelerate prend le relais et vous en êtes averti. Si l'incident peut être résolu par l'opérateur récepteur, des mesures sont prises pour le résoudre rapidement. Les opérateurs d'AMS Accelerate consultent la documentation interne pour trouver une solution et, si nécessaire, transmettent l'incident à d'autres ressources de support jusqu'à ce qu'il soit résolu. Une fois le problème résolu, l'équipe opérationnelle d'AMS Accelerate documente l'incident et sa résolution pour une utilisation future.

Dans les cas où des incidents graves ont un impact sur vos charges de travail critiques, AMS Accelerate peut recommander une restauration de l'infrastructure. Il faut souvent trouver un compromis entre le dépannage d'un problème et la simple restauration à partir d'une sauvegarde fonctionnelle connue. Les risques et les impacts des interruptions de service sont les facteurs

décisifs. Si vous avez du temps à consacrer à la résolution des problèmes, AMS Accelerate vous aidera, et votre responsable de prestation de services cloud (CSDM) peut intervenir, mais si l'urgence de la restauration est élevée, AMS Accelerate peut lancer une restauration immédiatement.

Gestion des incidents dans AMS Accelerate

Depuis AWS le Centre de support, vous pouvez effectuer les tâches suivantes :

- Signalez et mettez à jour un incident. Pour signaler un incident AMS Accelerate, choisissez AMS Operations -- Signaler un incident dans le menu Services.
- Obtenez une liste et des informations détaillées sur tous les incidents que vous avez soumis.
- Affinez votre recherche d'incidents en fonction de leur statut et d'autres filtres.
- Ajoutez des communications et des pièces jointes à vos incidents, et ajoutez des destinataires par e-mail pour la correspondance des dossiers.
- Lancez un chat en direct ou demandez à être rappelé à propos de votre incident.

> **Note**
>
> La fonctionnalité de chat en direct n'est pas destinée aux événements de sécurité ; pour les problèmes de sécurité, créez un dossier d'assistance prioritaire (P1 ou P2).

- Résolvez les incidents.
- Évaluez les communications relatives aux incidents.

Les exemples suivants décrivent l'utilisation du Centre de Support pour soumettre un incident. Une fois l'incident soumis, l'équipe AMS Accelerate travaille avec vous pour résoudre l'incident conformément au SLA standard AMS Accelerate.

Soumission d'un incident pour Accelerate

Pour signaler un incident à l'aide du Centre de support, reportez-vous à la documentation d'assistance : Création d'un dossier de support

Pour signaler un incident à l'aide Support du centre :

1. Cliquez sur Créer un dossier. La page de création d'un dossier d'incident s'ouvre.
2. Ouvrez le menu Type de problème du support technique et choisissez AMS Operations -- Signaler un incident. Fournissez des informations sur votre incident et choisissez Create.

3. Pour être tenu informé par e-mail à chaque étape du processus de résolution d'un incident, assurez-vous de remplir l'option CC Emails ; si vous vous connectez par fédération, connectez-vous avant de suivre le lien contenu dans l'e-mail qu'AMS Accelerate vous envoie à propos de l'incident.

> **Note**
>
> Votre description doit être aussi détaillée que possible. Incluez des informations pertinentes sur les ressources, ainsi que tout autre élément susceptible de nous aider à comprendre votre demande. Par exemple, pour la résolution de problèmes liés aux performances, incluez des horodatages et des journaux. Pour des demandes de fonctionnalités ou des questions d'ordre général, incluez une description de votre environnement et votre objectif. Dans tous les cas, suivez les conseils pour la description qui s'affichent sur votre formulaire de soumission de demande.
> En fournissant le plus de détails possible, vous augmentez les chances de résolution rapide de votre problème.

Vous pouvez également utiliser l'API AWS Support avec le code de service `service-ams-operations-report-incident` pour signaler un incident.

Surveillance et mise à jour d'un incident Accelerate

Vous pouvez mettre à jour, surveiller et examiner les rapports d'incidents et les demandes de service, tous deux appelés cas, en utilisant le Centre de support ou par programmation à l'aide de l' Support API, `DescribeCases`opération.

Pour suivre un dossier, un incident ou une demande de service à l'aide de Support Center, procédez comme suit.

1. Dans la console AWS de gestion, accédez à Support.
2. Dans le menu de navigation de gauche, sélectionnez Vos dossiers d'assistance, naviguez jusqu'à un dossier et cliquez sur le lien Objet pour ouvrir une page détaillée avec l'état actuel et les correspondances.

   Si vous souhaitez utiliser le téléphone ou le chat à ce stade, cliquez sur Ouvrir le dossier dans le Centre de support pour ouvrir la page de création de dossier dans le Support Centre, renseignée automatiquement avec le type de service AMS.

Lorsqu'un incident signalé ou une demande de service est mis à jour par l'équipe des opérations d'Accelerate, vous recevez un e-mail et un lien vers l'incident dans le Centre de Support afin que vous puissiez y répondre.

> **Note**
>
> Vous ne pouvez pas répondre à la correspondance concernant un dossier en répondant à l'e-mail.

S'il existe de nombreux cas dans le tableau de bord, vous pouvez utiliser l'option Filtrer :

- Objet : utilisez ce filtre pour effectuer une recherche par mots clés dans l'objet du dossier.
- Gravité : utilisez cette option pour filtrer les cas par gravité en sélectionnant une gravité dans la liste.
- Type de dossier : utilisez cette option pour voir tous les cas d'un type de cas particulier. Les incidents accélérés et les demandes de service apparaissent sous le type de dossier de support technique, ainsi que tous les cas spécifiques au service.
- État : utilisez cette option pour filtrer les dossiers par statut en sélectionnant un statut spécifique dans la liste.

3. Pour vérifier l'état le plus récent, actualisez la page.
4. Si le nombre de correspondances est tel qu'elles n'apparaissent pas toutes sur la page, choisissez Load More.
5. Pour fournir une mise à jour de l'état du dossier, choisissez Répondre, entrez la nouvelle correspondance, puis choisissez Soumettre.
6. Pour clôturer le dossier une fois qu'il a été résolu à votre satisfaction, choisissez Fermer le dossier.

   N'oubliez pas de donner une note de 1 à 5 étoiles au service pour faire savoir à AMS comment nous nous en sortons.

Gérer les incidents Accelerate avec l'API de support

Vous pouvez utiliser l'Support API pour créer des incidents et ajouter de la correspondance avec Support le personnel lors des enquêtes sur vos problèmes. L' Support API modélise une grande partie du comportement du AWS Support Center.

Pour plus d'informations sur l'utilisation de ce service d' AWS assistance, voir Programmation de la durée de vie d'un dossier de AWS support.

> **Note**
>
> L'équipe AMS Accelerate reçoit les incidents que vous avez créés par programmation à l'aide du code de service with. `service-ams-operations-report-incident`

Répondre à un incident généré par AMS Accelerate

AMS Accelerate surveille vos ressources de manière proactive. Pour plus d'informations, consultez Surveillance et gestion des événements dans AMS Accelerate. Il arrive qu'AMS Accelerate identifie et crée un incident, le plus souvent pour vous avertir d'un événement. Si une action de votre part est requise pour résoudre un incident, une notification est envoyée par l'équipe AMS Accelerate aux coordonnées que vous avez fournies pour le compte. Vous répondez à cette notification de la même manière que pour tout autre incident, généralement par le biais du Centre de Support, bien que dans certains cas, un contact par e-mail ou par téléphone soit nécessaire.

> **Important**
>
> Pour recevoir des notifications de changement d'état suite à un incident ou à une demande de service, entrez une adresse e-mail dans le champ des adresses.

Regardez la vidéo d'Akshay pour en savoir plus (4:15)

Gestion des demandes de service dans Accelerate

Rubriques

- Quand utiliser une demande de service pour Accelerate

- Comment fonctionne la gestion des demandes de service dans Accelerate
- Création d'une demande de service dans Accelerate
- Surveillance et mise à jour d'une demande de service pour Accelerate
- Gestion des demandes de service avec l'API de support pour Accelerate
- Répondre à une demande de service générée par AMS Accelerate

AMS Accelerate utilise la gestion des demandes de service pour enregistrer, agir, communiquer la progression des demandes de service et fournir des notifications en cas de demandes de service actives.

L'objectif du processus de gestion des demandes de service est de garantir que votre service géré fournit ce dont vous avez besoin.

Pour les requêtes liées à la facturation, créez une demande de service.

> **Note**
>
> L'équipe AMS Accelerate reçoit les demandes de service que vous avez créées par programmation à l'aide de l'API AWS Support avec le code de service. `service-ams-operations-service-request`

À l'aide du Centre de support AWS, vous pouvez effectuer les tâches suivantes :

- Signalez et mettez à jour une demande de service. Pour une demande de service AMS Accelerate, choisissez AMS Operation -- Service Request dans le menu Services.
- Obtenez une liste et des informations détaillées sur toutes les demandes de service que vous avez soumises.
- Affinez votre recherche de demandes de service en fonction du statut et d'autres filtres.
- Ajoutez des communications et des pièces jointes à vos demandes, et ajoutez des destinataires par e-mail pour la correspondance des dossiers.
- Résolvez les demandes de service.
- Communications relatives aux demandes de service tarifaire.

Quand utiliser une demande de service pour Accelerate

Les exemples suivants décrivent une demande de service. Une fois que vous avez soumis une demande de service, l'équipe AMS Accelerate travaille avec vous pour résoudre la demande conformément à votre accord de niveau de service AMS.

- AMS ou conseils AWS généraux
- Questions relatives à Patch MW
- Questions relatives au calendrier de sauvegarde
- Questions relatives à la fonctionnalité des AWS services

Voici des exemples de ce qui ne devrait pas être indiqué dans une demande de service :

- Problèmes d'accès
- Défaillance du correctif
- Défaillance de sauvegarde

Comment fonctionne la gestion des demandes de service dans Accelerate

Les demandes de service sont traitées par l'équipe opérationnelle d'AMS Accelerate sur appel.

Une fois que votre demande de service est reçue par l'équipe opérationnelle d'AMS Accelerate, elle est examinée pour s'assurer qu'elle est correctement classée comme une demande de service ou un incident. S'il est reclassé en tant qu'incident, le processus de gestion des incidents AMS Accelerate démarre et vous recevez une notification.

Si l'opérateur AMS Accelerate parvient à résoudre la demande de service, les mesures nécessaires sont prises immédiatement. Par exemple, si la demande de service concerne des conseils d'architecture ou d'autres informations, l'opérateur vous oriente vers les ressources appropriées ou répond directement à la question.

Si l'analyse de votre demande de service identifie un bogue ou une demande de fonctionnalité, AMS vous envoie une notification par le biais de la demande de service. Comme il n'y a pas d'heure limite pour les demandes de fonctionnalités ou les corrections de bogues, la demande de service initiale est close. Contactez votre CSDM pour les questions de suivi relatives à la demande de service initiale.

Si la demande de service n'est pas couverte par les opérations AMS Accelerate, l'opérateur envoie la demande à votre responsable de prestation de services cloud, afin qu'il puisse communiquer avec

vous, ou à l'équipe d' AWS assistance appropriée, accompagnée d'un e-mail vous indiquant les mesures prises.

La demande de service n'est pas résolue tant que vous n'avez pas indiqué que vous êtes satisfait du résultat.

> **Note**
>
> Nous vous recommandons de fournir une adresse e-mail, un nom et un numéro de téléphone de contact dans tous les cas afin de faciliter les communications.

Création d'une demande de service dans Accelerate

Pour créer une demande de service, procédez comme suit :

1. Depuis la console AMS Accelerate, accédez au tableau de bord.
2. Choisissez Ouvrir une demande de service, l'AMS — Demande de service est présélectionnée.
3. Choisissez une catégorie.
4. Choisissez Severity (niveaux Plus ou Premium uniquement).
5. Entrez les informations pour :
   - Objet : titre descriptif de la demande de service.
   - Description : description complète de la demande de service, des systèmes concernés et du résultat attendu d'une résolution.
6. Pour ajouter une pièce jointe, choisissez Joindre des fichiers,
   recherchez la pièce jointe souhaitée, puis sélectionnez Ouvrir.
   Pour supprimer la pièce jointe, cliquez sur l'icône de suppression
7. Contactez-nous : le contact par défaut AMS via le Web. Pour sélectionner d'autres options :
   - Langue de contact préférée : L'anglais est la langue prise en charge pour les demandes de service AMS Accelerate.
   - Web : Votre demande de service est soumise via le Web et traitée par l'équipe opérationnelle d'AMS.
   - Chat : discutez en ligne avec un représentant des opérations AMS Accelerate. Cette option vous ajoute à la file de discussion.

- Téléphone : Un représentant des opérations AMS vous rappelle. Entrez votre région AWS, votre numéro de téléphone et votre extension, le cas échéant.
- Contacts supplémentaires : entrez les adresses e-mail supplémentaires que vous souhaitez copier dans votre demande de service.

8. Sélectionnez Envoyer.

   Une page détaillée du dossier s'ouvre avec des informations sur la demande de service, telles que le type, l'objet, la création, l'identifiant et le statut. De plus, une zone de correspondance qui inclut la description de la demande que vous créez.

   Pour ouvrir une zone de correspondance et fournir des informations supplémentaires ou des mises à jour de statut, choisissez Répondre.

   Une fois la demande de service résolue, choisissez Résoudre le dossier.

   Si le nombre de correspondances est tel qu'elles n'apparaissent pas toutes sur la page, choisissez Load More.

   N'oubliez pas de donner une note de 1 à 5 étoiles au service pour faire savoir à AMS comment nous nous en sortons.

> **Note**
>
> Si vous souhaitez tester la fonctionnalité de demande de service, nous vous recommandons d'ajouter un indicateur de non-action à l'objet de votre demande de service, tel que`AMSTestNoOpsActionRequired`. Vous pouvez ensuite effectuer un test sans démarrer le processus de résolution des demandes de service.
> L'équipe AMS Accelerate reçoit les demandes de service que vous avez créées par programmation à l'aide de l'API AWS Support avec le code de service. `service-ams-operations-service-request`

Surveillance et mise à jour d'une demande de service pour Accelerate

Pour suivre un dossier, un incident ou une demande de service à l'aide de Support Center, procédez comme suit.

1. Dans la console AWS de gestion, accédez à Support.

2. Dans le menu de navigation de gauche, sélectionnez Vos dossiers d'assistance, naviguez jusqu'à un dossier et cliquez sur le lien Objet pour ouvrir une page détaillée avec l'état actuel et les correspondances.

   Si vous souhaitez utiliser le téléphone ou le chat à ce stade, cliquez sur Ouvrir le dossier dans le Centre de support pour ouvrir la page de création de dossier dans le Support Centre, renseignée automatiquement avec le type de service AMS.

   Lorsqu'un incident signalé ou une demande de service est mis à jour par l'équipe des opérations d'Accelerate, vous recevez un e-mail et un lien vers l'incident dans le Centre de Support afin que vous puissiez y répondre.

   > **Note**
   >
   > Vous ne pouvez pas répondre à la correspondance concernant un dossier en répondant à l'e-mail.

   Si le tableau de bord contient de nombreux cas, vous pouvez utiliser l'option Filtrer :

   - Objet : utilisez ce filtre pour effectuer une recherche par mots clés dans l'objet du dossier.
   - Gravité : utilisez cette option pour filtrer les cas par gravité en sélectionnant une gravité dans la liste.
   - Type de dossier : utilisez cette option pour voir tous les cas d'un type de cas particulier. Les incidents accélérés et les demandes de service apparaissent sous le type de dossier de support technique, ainsi que tous les cas spécifiques au service.
   - État : utilisez cette option pour filtrer les dossiers par statut en sélectionnant un statut spécifique dans la liste.
3. Pour vérifier l'état le plus récent, actualisez la page.
4. Si le nombre de correspondances est tel qu'elles n'apparaissent pas toutes sur la page, choisissez Load More.
5. Pour fournir une mise à jour de l'état du dossier, choisissez Répondre, entrez la nouvelle correspondance, puis choisissez Soumettre.
6. Pour clôturer le dossier une fois qu'il a été résolu à votre satisfaction, choisissez Fermer le dossier.

N'oubliez pas de donner une note de 1 à 5 étoiles au service pour faire savoir à AMS comment nous nous en sortons.

Gestion des demandes de service avec l'API de support pour Accelerate

Vous pouvez utiliser l'API AWS Support pour créer des demandes de service et y ajouter de la correspondance tout au long des enquêtes sur vos problèmes et des interactions avec le personnel de AWS support. L'API de AWS support modélise une grande partie du comportement du centre de AWS support.

L'équipe AMS reçoit également les demandes de service que vous avez créées par programmation à l'aide de l'API AWS Support avec le code service-ams-operations-service de service -request.

Pour plus d'informations sur la manière dont vous pouvez utiliser ce service d' AWS assistance, voir Programmation de la durée de vie d'un dossier de AWS support.

Répondre à une demande de service générée par AMS Accelerate

AMS Accelerate surveille vos ressources de manière proactive ; pour plus d'informations, consultezSurveillance et gestion des événements dans AMS Accelerate. AMS Accelerate crée parfois une demande de service ou une notification de service pour vous, généralement si une action de votre part est requise pour résoudre une demande de service. Dans ce cas, l'équipe AMS Accelerate envoie une notification au contact que vous avez indiqué pour le compte. Vous répondez à cette demande de service de la même manière que dans tous les autres cas, généralement par le biais du Centre de support, bien que dans certains cas, une correspondance par e-mail ou par téléphone soit requise.

> **Important**
>
> Pour recevoir des notifications de changement d'état pour une demande de service ou un cas d'incident, vous devez avoir saisi une adresse e-mail dans le champ des adresses. Les notifications sont envoyées uniquement à l'adresse e-mail ajoutée au dossier lors de sa création.

Le lien contenu dans l'e-mail de notification ne fonctionne que si vous utilisez un serveur de messagerie sur votre réseau fédéré AMS Accelerate. Sinon, vous pouvez répondre à la

correspondance en accédant à votre console AMS Accelerate et en utilisant la page des détails du dossier.

> **Note**
>
> AMS Accelerate envoie les communications à votre adresse e-mail principale associée à votre AWS compte ; nous vous recommandons d'ajouter un autre alias d'e-mail de contact opérationnel afin de faciliter le processus request/notification de gestion des services. Cela est abordé lors du processus d'intégration d'AMS Accelerate et dans la documentation d'intégration associée.

Test des rapports d'incidents et des demandes de service dans Accelerate

Lorsque vous testez des rapports d'incidents ou des demandes de service, nous vous demandons de les inclure AMSTestNoOpsActionRequireddans le texte d'objet. Cela permet à AMS de savoir que l'incident ou la demande est uniquement destiné à des tests. Lorsque les ingénieurs des opérations d'AMS le verront, ils ne réagiront en aucune façon.

Questions relatives à la facturation pour AMS Accelerate

Pour soumettre une question relative à la facturation, procédez comme suit :

1. Ouvrez le AWS Support centre à la https://console.aws.amazon.com/support/ maison#/.
2. Choisissez Compte et facturation.
3. Choisissez Create case (Créer une demande).
4. Choisissez Compte et facturation, puis suivez les instructions pour soumettre votre dossier.

Gestion des événements planifiés dans AWS Managed Services

La gestion des événements planifiés (PEM) d'AWS Managed Services (AMS) est une offre de services AMS. PEM engage, coordonne et assiste lors d'événements et de projets clients à l'aide des services AMS. Le PEM aide à coordonner un ensemble d'activités connexes qui correspondent à la portée et au calendrier convenus de l'événement ou du projet PEM.

Critères AMS PEM

Un événement planifié est un projet dont la portée et le temps sont limités. AMS utilise les informations que vous fournissez (y compris le plan et le champ d'application, les résultats attendus et les modifications que les opérations d'AMS sont censées apporter) pour vous aider efficacement lors de vos activités PEM. Vos architectes cloud (CAs) examinent et évaluent ensuite l'intégralité de l'activité PEM, la mise en œuvre technique et l'engagement des opérations AMS. Après examen par CA, AMS Operations examine les plans et assure la coordination avec votre responsable de la prestation de services cloud (CSDM) pour l'engagement de l'équipe opérationnelle.

Types de PEM

Les types PEM disponibles sont les suivants :

- Journées de jeu
  - Operational Gameday : approche ludique basée sur des scénarios pour la réponse opérationnelle, visant à valider l'intégration des processus, des personnes et des systèmes.
  - Security Gameday : stratégie de réponse aux incidents de sécurité qui utilise une approche de jeu basée sur des scénarios pour évaluer l'intégration des systèmes, des processus et du personnel.
- Événement lié à la sécurité du client : événements de sécurité planifiés. Par exemple, les tests de pénétration.
- Support à la migration : support pour les activités d'intégration et de migration planifiées.

Ce flux de travail facilite la collaboration avec AMS pour coordonner les événements planifiés et les activités de migration concernant le support AMS. Pour obtenir de l'aide concernant vos besoins spécifiques, contactez votre CSDM.

Le processus AMS PEM

Le processus PEM comprend les phases suivantes :

- Initiation au PEM : vous travaillez avec votre CSDM pour définir votre objectif pour l'événement prévu et déterminer ce dont les opérations d'AMS ont besoin. AMS CAs examine les aspects techniques du plan PEM. Le CAs travail avec AMS Security and Operations sur la conformité, l'optimisation de l'exécution et l'automatisation, ainsi que pour définir les tâches et les livrables avant l'exécution du PEM. Ensuite, votre CSDM crée le ticket PEM et fournit à AMS les informations du projet et les détails techniques. AMS a besoin d'un délai de 14 jours calendaires pour permettre à l'équipe des opérations AMS de planifier, de fournir un examen technique et d'affecter les ressources.
- Révision PEM : L'équipe des opérations AMS examine la demande PEM et travaille avec votre CSDM pour vérifier que les informations du plan PEM sont correctes et complètes.
- Acceptation du PEM : AMS examine les informations fournies et communique au CSDM quel sera le niveau de soutien pendant l'activité PEM. Si le PEM contient des informations complètes et que votre CSDM est d'accord avec l'étendue des travaux, le PEM est approuvé.
- Préparation et exécution : AMS s'assure que les tâches nécessaires avant le début du PEM sont terminées et facilite les communications internes et avec les clients. AMS s'assure que le plan PEM fonctionne correctement et fournit des rapports d'état et de progression.

PEM FAQs

Comment puis-je contacter AMS via Cases : Service Request (SRs) /Incident lors d'un événement PEM ?

- Utilisez l'ID PEM partagé par votre CSDM dans la ligne d' RFC/SR objet du format. `PEM-ID`

  Le cas échéant, vous pouvez utiliser l'option Contact en direct.
- Vous pouvez également créer une demande de service (SR) pour discuter de vos cas d'utilisation ou pour toute question concernant votre événement prévu. Si vous utilisez un SR, le PEM n'a pas besoin d'être valide.

Quelles sont les validations effectuées lorsqu'un dossier lié au PEM est soumis ?

- Vérification que l'identifiant du compte figure sur le PEM.

- Vérification que le statut PEM est approuvé et actif entre les dates de début et de fin fournies.
- Un lien vers les détails du PEM est fourni en interne aux ingénieurs d'AMS.

Existe-t-il SLAs ou SLOs pour des demandes PEM ?

- PEMs ne sont pas associés à SLAs ou SLOs.
- SLAs et SLOs pour les tâches liées au PEM (demande de service, incidents), elles sont définies par AMS. SLOs

  Pour plus d'informations, consultez les rapports d'incidents, les demandes de service et les questions de facturation dans AMS Accelerate.

Pouvons-nous créer un PEM via une demande de service (SR) ?

- Non, la création de PEM doit être gérée par le Cloud Service Delivery Manager (CSDM).

Opérations à la demande

Operations on Demand (OOD) est une fonctionnalité d'AWS Managed Services (AMS) qui étend le champ d'application standard de votre plan d'opérations AMS en fournissant des services opérationnels qui ne sont pas actuellement proposés nativement par les plans d'opérations AMS ou AWS. Une fois sélectionnée, l'offre de catalogue est fournie grâce à une combinaison d'automatisation et de ressources AMS hautement qualifiées. Il n'y a aucun engagement à long terme ni aucun contrat supplémentaire, vous permettant d'étendre votre AMS existant ainsi que vos AWS opérations et capacités selon vos besoins. Vous acceptez d'acheter des blocs d'heures (blocs OOD), 20 heures par bloc, sur une base mensuelle.

Vous pouvez effectuer une sélection dans le catalogue d'offres standardisées et initier un nouvel engagement OOD par le biais d'une demande de service. Parmi les offres OOD, citons l'assistance à la maintenance d'Amazon EKS, à l' AWS Control Tower exploitation et à la gestion des clusters SAP. De nouvelles offres de catalogue sont ajoutées régulièrement en fonction de la demande et des cas d'utilisation opérationnels les plus courants.

L'OOD est disponible pour les plans d'exploitation AMS Advanced et AMS Accelerate et est disponible partout Régions AWSoù AMS est disponible.

AMS assure la gestion des risques liés à la sécurité des clients (CSRM) tout en mettant en œuvre les modifications que vous avez demandées. Pour en savoir plus sur le processus CSRM, consultez la section Révisions de sécurité des demandes de modification.

Catalogue d'offres Operations on Demand

Operations on Demand (OOD) vous propose les services décrits dans le tableau suivant.

> **Note**
>
> Pour les définitions des termes clés, reportez-vous à la documentation d'AWS Managed Services Key Terms.

Plan des opérations	Titre	Description	Résultats attendus

AMS Accelerate	Maintenance du cluster Amazon EKS	AMS libère vos développeurs de conteneurs en gérant la maintenance continue de vos déploiements Amazon Elastic Kubernetes Service (Amazon EKS). AMS exécute les end-to-end procédures nécessaires pour mettre à jour un cluster en abordant les composants du plan de contrôle, des modules complémentaires et des nœuds. AMS effectue la mise à jour des types de nœuds gérés ainsi que d'un ensemble sélectionné de modules complémentaires Amazon EKS et Kubernetes.	Les équipes du client ont participé aux opérations sous-jacentes de mise à jour des clusters Amazon EKS.

AMS Accelerate	Bâtiment AMI et distributeurs automatiques	AMS assure la gestion continue de la création et de la distribution automatique d'AMI pour les clients. Nos ingénieurs publient une version mensuelle des versions par abonnement AMIs, publient des versions à la demande AMIs pour les activités de correction émergentes, gèrent les modificat ions à l'aide de runbooks et surveillent les builds d'AMI à l'aide de Monitoring. CloudWatc h Nous fournissons également une assistance au dépannage et des rapports détaillés pour tous les comptes AMIs utilisés dans des comptes désignés. Cette offre nécessite le déploiement de pipelines de génération d'AMI via le générateur EC2 d'images. AMS ne prend en charge aucun autre service ou automatisation interagis sant avec EC2 Image Builder.	Le niveau de sécurité des clients s'est amélioré et le temps passé par les clients à construir e et à vendre a été AMIs réduit.

AMS Accelerate	Exécution des modifications organisée	Travaillez avec nos ingénieurs d'exploitation qualifiés pour traduire les exigences de votre entrepris e en demandes de modification validées pouvant être exécutées en toute sécurité dans votre AWS environnement. Profitez de notre approche unique en matière d'automatisation et de notre connaissance des meilleure s pratiques opérationnelles (par exemple, évaluation d'impact, annulations, règle des deux personnes), qu'il s'agisse d'un simple changement à grande échelle ou d'une action complexe ayant des impacts en aval.	Les clients ont participé à la définitio n, à la création et à l'exécution de demandes de modification personnalisées. Les modificat ions peuvent être manuelles ou automatis ées (CloudFor mationSSM). Comprend une consultation Support pour obtenir des conseils de configura tion si nécessaire. Non destiné aux modifications du code de l'applica tion, à l'installation/ au déploiement d'applications, à la migration des données ou aux modifications de configuration du système d'exploit ation.

AMS Accelerate	AWS Network Firewall Opérations	AMS collabore avec vous pour intégrer votre pare-feu et mettre en œuvre et gérer les politiques et les règles relatives aux opération s continues du pare-feu. Pour ce faire, nos ingénieurs tirent parti de nos meilleures pratiques opération nelles et de notre automatisation pour configurer des politiques et des règles standardisées, et en activant la surveillance afin de détecter les modifications apportées en dehors du processus d'automatisation. AMS vous avertit rapidement des modificat ions indésirables et propose des options permettant de les inclure, sur demande, ou de rétablir la configuration précédente du compte afin de garantir la stabilité globale de vos systèmes.	Les équipes clients ont contribué à réduire les frais de gestion en détectant rapidemen t les modificat ions involonta ires du pare-feu réseau, ce qui a permis d'amélior er la résolution des incidents et de réduire le temps d'analyse des causes profondes des problèmes attendus et inattendu s.
AMS Accelerate	AWS Control Tower opération s	Exploitation et gestion continues de votre zone AWS Control Tower d'atterrissage, y compris AWS Transit Gateway, et AWS Organizat ions fourniture d'une solution complète de zone d'atterrissage. Nous gérons la vente de comptes, la gestion des SCP et des unités d'organisation, la correction des dérives, la gestion des utilisateurs SSO et les AWS Control Tower mises à niveau grâce à notre bibliothèque de commandes et de garde-corps personnalisés.	Les équipes clients ont participé à certaines des opérations sous-jacentes liées à la gestion AWS Control Tower, à AWS Transit Gateway et AWS Organizations.

AMS Accelerate	AWS zone d'atterrissage Accélérer les opérations	AMS assure l'exploitation continue des zones d' AWS atterrissage déployées via AWS Landing Zone Accelerator (LZA). Nos ingénieurs s'occupent des modifications des fichiers de configuration, AWS Control Tower de la gestion de l'environnement (vente de comptes, création d'unités d'organisation, garde-fou s CT), de la gestion des politique s de contrôle des services (SCP), de la détection et de la correction de la dérive CT, de la gestion de la configuration réseau et des mises à jour du framework CT et LZA. AWS LZA fournit un moyen de configure r et de gérer un AWS environne ment multi-comptes sécurisé en utilisant les meilleures pratiques opérationnelles et des services tels que. AWS Control Tower	Les équipes du client ont participé aux opérations continues et à la gestion de la solution AWS Landing Zone Accelerator.

AMS Accelerate	SAP Cluster Assist	Alarme, surveillance, correction de clusters, sauvegarde et résolution des incidents dédiés pour vos clusters SAP. Cet élément du catalogue vous permet de déléguer une partie du travail opérationnel en cours à votre équipe des opérations SAP afin qu'elle puisse se concentrer sur la gestion des capacités et le réglage des performances.	Les équipes SAP du client ou du partenaire ont participé à certaines des opérations sous-jacentes. Le client doit toujours fournir d'autres fonctionnalités SAP, telles que la gestion des capacités, le réglage des performances, le DBA et l'administration de base SAP.

AMS Accelerate	SQL Server sur les EC2 opérations	AMS collabore avec vous pour intégrer, implémenter et gérer les opérations continues de vos bases de données SQL Server déployées sur EC2 des instances. Nos ingénieurs tirent parti de nos meilleures pratiques opération nelles et de notre automatisation pour libérer vos équipes de base de données en effectuant des tâches telles que la sauvegarde et l'application de correctifs, en étendant le support opérationnel d'AMS aux correctifs SQL Server pour inclure des mises à jour continues adaptées aux clusters, des services de sauvegarde et de restauration conformes à notre stratégie de défense contre les ransomwares, et en surveillant le respect des contrôles de sauvegard e et de correction fournis par le client.	Les clients de SQL Server ont aidé à décharger les opérations de correction et de sauvegarde des bases de données afin d'améliorer la résilience et le niveau de sécurité de leurs charges de travail, en plus d'optimiser les coûts de licence en apportant leurs propres licences (BYOL) à. EC2

AMS avancé	Maintenance du cluster Amazon EKS	AMS libère vos développeurs de conteneurs en gérant la maintenance continue et l'intégrité de vos déploiements Amazon Elastic Kubernetes Service (Amazon EKS). AMS exécute les end-to-end procédures nécessaires pour mettre à jour un cluster en abordant les composants du plan de contrôle, des modules complémentaires et des nœuds. AMS effectue la mise à jour des types de nœuds gérés ainsi que d'un ensemble sélectionné de modules complémentaires Amazon EKS et Kubernetes.	Les équipes du client ont participé aux opérations sous-jacentes de mise à jour des clusters Amazon EKS.
AMS avancé	Exécution RFC prioritaire	Capacité d'ingénieur des opérations AMS désignée pour prioriser l'exécution de vos demandes de changement (RFC). Toutes les soumissions reçoivent un niveau de réponse plus élevé et l'ordre de priorité peut être ajusté en interagissant directement avec les ingénieurs via une salle de réunion Amazon Chime.	Les clients reçoivent un délai de réponse de 8 heures pour RFCs.

AMS Advanced et AMS Accelerate	Mise à niveau de l'ancien système	Évitez une migration d'instance en mettant à niveau les instances vers une version de système d'exploitation prise en charge. Nous pouvons effectuer une mise à niveau sur place sur les instances que vous avez sélectionnées en tirant parti de l'automatisation et des capacités de mise à niveau des fournisseurs de logiciels (par exemple, Microsoft Windows 2008 R2 vers Microsoft Windows 2012 R2). Cette approche est idéale pour les applications existantes qui ne peuvent pas être facilement réinstallées sur une nouvelle instance et fournit une protection supplémentaire contre les menaces de sécurité connues et non atténuées sur les anciennes versions du système d'exploitation. Les systèmes d'exploitation suivants sont pris en charge pour les mises à niveau sur place : • Microsoft Windows 2012 R2 vers Microsoft Windows 2016 et versions ultérieures • Microsoft Windows 2016 à Microsoft Windows 2022 et versions ultérieures • Red Hat Enterprise Linux 7 vers Red Hat Enterprise Linux 8 • Red Hat Enterprise Linux 8 vers Red Hat Enterprise Linux 9	Cette solution est fournie pour les applications qui ne peuvent plus être réinstallées sur une nouvelle instance (par exemple, perte de code source, faillite d'un éditeur de logiciels indépendants, etc.). Vous pouvez rétablir les mises à niveau qui ont échoué dans leur état d'origine. D'un point de vue opérationnel, il est préférable de revenir en arrière, car cela permet de rendre l'instance plus facile à prendre en charge avec les derniers correctifs de sécurité.

		• Oracle Linux 7 vers Oracle Linux 8	

Rubriques

- Demande d'opérations AMS à la demande
- Apporter des modifications aux offres d'opérations à la demande

Demande d'opérations AMS à la demande

AWS Managed Services (AMS) Operations on Demand (OOD) est disponible pour tous Comptes AWS ceux qui ont été intégrés à AMS. Pour tirer parti d'Operations on Demand, demandez des informations supplémentaires à votre responsable de prestation de services cloud (CSDM), à votre architecte de solutions (SA), à votre responsable de compte ou à votre architecte cloud (CA). Les offres OOD disponibles sont répertoriées dans le tableau précédent du catalogue des offres Operations on Demand. Une fois le cadrage de l'engagement terminé, soumettez une demande de service à AMS Operations pour initier un engagement pour OOD.

Chaque demande de service OOD doit contenir les informations détaillées suivantes relatives à l'engagement :

- Les offres OOD spécifiques demandées, et pour chaque offre OOD spécifique :
  - Le nombre de blocs (un bloc est égal à 20 heures de temps de ressources opérationnelles au cours d'un mois civil donné, à facturer au AWS tarif standard alors en vigueur pour l'offre Operations on Demand applicable) à allouer à l'offre OOD spécifique.
  - L'ID de compte pour chaque compte AWS Managed Services pour lequel l'offre OOD spécifique est demandée.

Les demandes de service OOD doivent être soumises par vous par le biais de :

- Le compte AWS Managed Services qui reçoit les offres Operations on Demand applicables, ou
- Un compte AWS Managed Services qui est un compte de AWS Organizations gestion en mode toutes fonctionnalités, au nom de tous ses comptes membres qui sont des comptes AWS Managed Services.

Une fois la demande de service OOD reçue, AMS Operations examine et met à jour les comptes avec leur approbation, leur approbation partielle ou leur refus.

Une fois que la demande de service des offres OOD est approuvée, AMS et vous coordonnez le début de l'engagement. Aucune offre OOD n'est lancée tant que la demande de service n'est pas approuvée et qu'une date de début d'engagement n'est pas convenue.

AMS utilise une allocation d'abonnement mensuelle de blocs OOD. Nous allouons le nombre de blocs approuvé chaque mois, à compter de la date de début de l'engagement, jusqu'à ce que vous demandiez de vous désinscrire par le biais d'une nouvelle demande de service. Les blocs OOD sont valables pendant un mois civil. Les blocs, ou portions de blocs, non utilisés ne sont ni reportés ni reportés aux mois futurs.

Vous êtes facturé au moins un bloc OOD par mois, quel que soit le nombre d'heures réellement utilisées. Tout bloc OOD supplémentaire alloué dans lequel aucune heure n'a été utilisée n'est pas facturé.

Apporter des modifications aux offres d'opérations à la demande

Pour demander des modifications aux engagements en cours pour les offres d'opérations à la demande (OOD), soumettez une demande de service contenant les informations suivantes :

- La ou les modifications demandées, et
- Date demandée pour que les modifications entrent en vigueur.

Après avoir reçu la demande de service OOD, AMS Operations examine la demande et la met à jour avec son approbation ou demande que le CSDM désigné travaille avec vous pour déterminer la portée et les implications de la modification. S'il est déterminé que la modification nécessite un effort de cadrage auprès du CSDM, vous devez soumettre une deuxième demande de service OOD pour lancer l'engagement modifié une fois l'exercice de cadrage terminé.

Une fois approuvée, l'allocation de blocs la plus récemment modifiée devient et reste active, remplaçant toutes les allocations de blocs précédentes, sauf accord contraire entre vous AWS et vous.

Rapports et options

AWS Managed Services (AMS) rassemble les données de différents services AWS natifs afin de fournir des rapports à valeur ajoutée sur les principales offres AMS.

AMS propose deux types de rapports détaillés :

- Rapports sur demande : vous pouvez demander certains rapports ad hoc par le biais de votre Cloud Service Delivery Manager (CSDM). Ces rapports ne sont pas limités, car vous devrez peut-être les demander plusieurs fois lors de l'intégration ou lors d'événements critiques. Sachez toutefois que ces rapports ne sont pas conçus pour être fournis selon un calendrier tel que les rapports hebdomadaires. Pour mieux comprendre vos besoins ou pour plus d'informations sur l'utilisation des rapports en libre-service, contactez votre CSDM.
- Rapports en libre-service : les rapports en libre-service AMS vous permettent d'interroger et d'analyser directement les données aussi souvent que vous le souhaitez. Utilisez des rapports en libre-service pour accéder aux rapports depuis la console AMS et des ensembles de données de rapports via des compartiments S3 (un compartiment par compte). Cela vous permet d'intégrer les données dans votre outil de Business Intelligence (BI) préféré afin de personnaliser les rapports en fonction de vos besoins.

Rubriques

- Rapports sur demande
- Rapports en libre-service

Rapports sur demande

Rubriques

- Rapports de gestion des hôtes AMS
- Rapports AMS Backup
- AWS Config Rapport de conformité des contrôles
- Rapport de configuration des réponses aux règles de configuration AMS Config
- Incidents évités et suivi des rapports Top Talkers
- Rapport détaillé sur les frais de facturation

- Rapports Trusted Remediator

AMS rassemble les données de divers services AWS natifs afin de fournir des rapports à valeur ajoutée sur les principales offres AMS. Pour obtenir une copie de ces rapports, adressez-vous à votre responsable de prestation de services cloud (CSDM).

Rapports de gestion des hôtes AMS

Rapports disponibles

- Rapport sur la couverture des agents SSM

Rapport sur la couverture des agents SSM

Le rapport de couverture de l'agent AMS SSM vous indique si l'agent SSM est installé ou non sur les EC2 instances du compte.

Nom du champ	Définition
Nom du client	Nom du client pour les situations où il existe plusieurs sous-clients
Région de ressources	AWS Région où se trouve la ressource
Nom du compte	Le nom du compte
AWS ID de compte	L'identifiant du AWS compte
ID de ressource	ID de l' EC2 instance
Nom de la ressource	Nom de l' EC2 instance
Drapeau conforme	Indique si l'agent SSM est installé sur la ressource (« Compliant ») ou non (« NON_COMPLIANT »)

Rapports AMS Backup

Rapports disponibles

- Backup Job Success/Rapport d'échec
- Rapport récapitulatif des sauvegardes
- Summary/Coverage Rapport de sauvegarde

Backup Job Success/Rapport d'échec

Le Success/Failure rapport Backup Job fournit des informations sur les sauvegardes effectuées au cours des dernières semaines. Pour personnaliser le rapport, spécifiez le nombre de semaines pour lesquelles vous souhaitez récupérer les données. Le nombre de semaines par défaut est de 12. Le tableau suivant répertorie les données incluses dans le rapport :

Nom du champ	Définition
ID de compte AWS	ID de compte AWS auquel appartient la ressource
Nom du compte	Nom du compte AWS
ID de la tâche de sauvegarde	L'ID de la tâche de sauvegarde
ID de ressource	L'ID de la ressource sauvegardée
Type de ressource	Type de ressource en cours de sauvegarde
Région de ressources	La AWS région de la ressource sauvegardée
État de la sauvegarde	État de la sauvegarde. Pour plus d'informations, consultez la section Statuts des tâches de sauvegarde
Identifiant du point de récupération	L'identifiant unique du point de récupération
Message d'état	Description des erreurs ou des avertissements survenus au cours de la tâche de sauvegarde
Taille de sauvegarde	Taille de la sauvegarde en Go
Point de récupération (ARN)	L'ARN de la sauvegarde créée

Nom du champ	Définition
Âge du point de récupération en jours	Nombre de jours écoulés depuis la création du point de récupération
Moins de 30 jours	Indicateur des sauvegardes datant de moins de 30 jours

Rapport récapitulatif des sauvegardes

Nom du champ	Définition
Nom du client	Nom du client pour les situations où plusieurs sous-clients sont
Mois de la sauvegarde	Mois de la sauvegarde
Année de sauvegarde	Année de la sauvegarde
Type de ressource	Type de ressource en cours de sauvegarde
Nombre de ressources	Le nombre de ressources sauvegardées
Nombre de points de récupération	Nombre d'instantanés distincts
Sauvegardes datant de moins de 30 jours	Nombre de sauvegardes datant de moins de 30 jours
Âge maximal des points de récupération	Le plus vieux point de guérison (âge en jours)
Âge minimum du point de récupération	Âge du point de récupération le plus récent en jours

Summary/Coverage Rapport de sauvegarde

Le Summary/Coverage rapport Backup indique le nombre de ressources qui ne sont actuellement protégées par aucun AWS Backup plan. Discutez avec votre CDSM d'un plan approprié pour augmenter la couverture, dans la mesure du possible, et pour réduire le risque de perte de données.

Nom du champ	Définition
Nom du client	Nom du client pour les situations où plusieurs sous-clients sont
Region (Région)	AWS région où se trouve la ressource
Nom du compte	Le nom du compte
AWS Identifiant du compte	L'identifiant du AWS compte
Type de ressource	Type de ressource. Les ressources sont prises en charge par AWS Backup (Aurora, DocumentDB, DynamoDB, EBS, EC2 EFS, RDS et S3) FSx
ARN des ressources	ARN de la ressource
ID de ressource	ID de la ressource
Couverture	Indique si la ressource est couverte ou non (« COVERED » ou « NOT_COVERED »)
Nombre de ressources	Nombre de ressources prises en charge dans le compte
perc_couverture	Pourcentage de ressources prises en charge dont une sauvegarde a été exécutée au cours des 30 derniers jours.

AWS Config Rapport de conformité des contrôles

Le rapport AWS Config Control Compliance fournit un examen approfondi de la conformité des ressources et des AWS Config règles des comptes AMS. Vous filtrez le rapport par gravité des règles de configuration pour hiérarchiser les résultats les plus critiques. Le tableau suivant répertorie les données fournies par ce rapport :

Champ	Description
Date	Date du rapport
Nom du client	Nom du client
AWS ID de compte	ID de AWS compte associé au client
Identifiant de source	AWS Config identifiant de source unique de la règle
Description de la règle	AWS Config description de la règle
Type de règle	AWS Config type de règle
Drapeau de conformité	AWS Config état de conformité des règles
Type de ressource	AWS type de ressource
Nom de la ressource	AWS nom de la ressource
Sévérité	Sévérité recommandée par défaut définie par AMS pour la AWS Config règle
Catégorie de remédiation	Catégorie de réponse de correction associée pour une règle AWS Config
Description des mesures correctives	Explication des mesures correctives pour assurer la AWS Config conformité de la règle
Action du client	Action du client requise pour garantir la conformité de la AWS Config règle
Rapport Delta Metrics	Modifications relatives à la conformité d'une règle entre deux dates données

Rapport de configuration des réponses aux règles de configuration AMS Config

Le rapport de configuration des réponses aux règles de configuration AMS fournit un aperçu détaillé de la manière dont Accelerate est actuellement configuré pour répondre aux règles de configuration AMS non conformes. Pour plus d'informations sur la façon de modifier la réponse pour les règles de configuration AMS, voir AMS Accelerate Customized findings responses.

Ce rapport indique uniquement les configurations que vous avez modifiées et exclut les configurations par défaut d'AMS répertoriées dans la bibliothèque de règles de configuration AMS. Le rapport fournit des données sur les ressources et la configuration des réponses aux règles de configuration AMS des comptes AMS, notamment les suivantes :

- Liste des AWS comptes pour lesquels vous avez modifié la réponse par défaut pour les règles de configuration AMS.
- Liste des balises auxquelles vous avez associé une réponse pour les règles de configuration AMS.
- La liste des configurations de réponse pour chaque règle, compte et tag.
- Liste des ressources pour lesquelles vous avez modifié la réponse par défaut pour les règles de configuration AMS.

Dernier rapport sur les configurations de réponse

Champ	Description
Date	Date à laquelle le rapport a été généré
Nom du client	Nom du client
AWS ID de compte	L'ID de AWS compte associé à la configuration
Nom du compte	AWS nom du compte du groupe de ressources au niveau du compte
Type de recherche	Type de découverte identifié. Dans ce cas, AWS Config

Champ	Description
Identifiant de source	AWS Config Identifiant de source unique de la règle
ID du groupe de ressources	L'ID du groupe de ressources associé à la configuration de la réponse
Action de réponse configurée	Type d'action déclenché par AMS
Runbook SSM associé	Le manuel de remédiation qui sera exécuté, le cas échéant
Type de groupe de ressources	Cela peut être un compte ou un tag

Ressources avec réponse par défaut personnalisée aux règles de configuration

Nom du champ	Définition
Nom du client	Nom du client
Date	Date à laquelle le rapport a été généré
AWS Nom du compte	AWS nom du compte
ID de compte	ID de AWS compte associé
Règle de configuration AMS	Règle de configuration AMS qui cible la ressource et s'applique à une configuration
ID de ressource	L'ID de ressource dans le compte client ciblé par la règle de configuration AMS
Région de ressources	La AWS région dans laquelle la configuration est appliquée
Type de ressource	AWS type de ressource

Nom du champ	Définition
ID du groupe de ressources	L'ID du groupe de ressources associé à la configuration de la réponse
Drapeau AMS de ressources	Si la AWS ressource est déployée par AMS, ce champ est défini sur `True`
Type de déclencheur	Type de réponse configuré pour la ressource
Drapeau de conformité	État de conformité aux règles de configuration AMS

Incidents évités et suivi des rapports Top Talkers

Rapports disponibles

- Rapport sur les incidents évités
- Rapport Monitoring Top Talkers

Rapport sur les incidents évités

Le rapport Incidents évités répertorie les CloudWatch alarmes Amazon qui ont été automatiquement corrigées, évitant ainsi un éventuel incident. Pour en savoir plus, consultez la section Correction automatique. Le tableau suivant répertorie les informations incluses dans ce rapport :

Nom du champ	Définition
Execution_start_time_utc	Date à laquelle l'automatisation a été exécutée
nom_client	Nom du client du compte
account_name	Le nom du compte
AwsAccountId	L'ID du compte AWS
nom_document	Le nom du document SSM ou de l'automat isation exécutée

Nom du champ	Définition
durée_en_minutes	Durée de l'automatisation en minutes
Region (Région)	AWS Région où se trouve la ressource
automation_execution_id	L'identifiant de l'exécution
statut d'exécution de l'automatisation	État de l'exécution

Rapport Monitoring Top Talkers

Le rapport Monitoring Top Talkers présente le nombre d' CloudWatch alertes Amazon générées au cours d'une période donnée et fournit des visualisations des ressources qui génèrent le plus grand nombre d'alertes. Ce rapport vous aide à identifier les ressources qui génèrent le plus grand nombre d'alertes. Ces ressources peuvent être utiles pour effectuer une analyse des causes premières afin de résoudre le problème ou pour modifier les seuils d'alarme afin d'éviter des déclenchements inutiles en l'absence de problème réel. Le tableau suivant répertorie les informations incluses dans ce rapport :

Nom du champ	Définition
Nom du client	Nom du client
AccountId	L'identifiant du AWS compte
Catégorie d'alerte	Type d'alerte déclenchée
Description	Description de l'alerte
ID de ressource	ID de la ressource qui a déclenché l'alerte
Nom de la ressource	Nom de la ressource qui a déclenché l'alerte
Region (Région)	AWS Région où se trouve la ressource
État de l'incident	Dernier état de l'incident généré par l'alarme
Première occurrence	Première fois que l'alerte a été déclenchée

Nom du champ	Définition
Événement récent	Heure à laquelle l'alerte a été déclenchée le plus récemment
Nombre d'alertes	Nombre d'alertes générées entre le premier événement et le plus récent

Rapport détaillé sur les frais de facturation

Le rapport détaillé des frais de facturation d'AWS Managed Services (AMS) fournit des informations détaillées sur les frais de facturation d'AMS avec les comptes associés et les services AWS correspondants, notamment :

- Frais de niveau de service AMS, pourcentages d'augmentation, niveaux de service AMS au niveau du compte et frais AMS.
- Comptes associés et frais AWS d'utilisation

Nom du champ	Définition
Mois de facturation	Le mois et l'année du service facturé
ID du compte du payeur	L'identifiant à 12 chiffres identifiant le compte qui sera responsable du paiement des frais AMS
ID du compte associé	L'identifiant à 12 chiffres identifiant le compte AMS qui consomme des services qui génèrent des dépenses
AWS Nom du service	Le AWS service qui a été utilisé
AWS Charges	Les AWS frais associés au nom du AWS service indiqué dans Nom du AWS service
Plan de tarification	Le nom du plan tarifaire associé au compte associé

Nom du champ	Définition
Proportion de levage	Le pourcentage d'augmentation (sous forme décimale V.WXYZ) basé sur pricing_plan, le SLA et le service AWS
AWS Charges ajustées	AWS utilisation ajustée pour AMS
Frais AWS augmentés	Pourcentage des frais AWS à facturer pour AMS ; adjust_aws_charges * uplift_percent
Instances : EC2 dépenses RDS	Dépenses consacrées EC2 aux instances RDS
Frais AMS	Total des frais AMS pour le produit ; uplifted_ aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp
Frais minimaux calculés au prorata	Le montant que nous facturons pour respecter le minimum contractuel
Frais minimaux	Frais minimaux d'AMS (le cas échéant)
Total des frais AMS du compte lié	Somme de tous les frais pour le link_account
Total des frais AMS du compte du payeur	Somme de tous les frais pour le compte du payeur

Rapports Trusted Remediator

Rapports disponibles

- Rapport récapitulatif de Trusted Remediator Remediation
- Rapport récapitulatif de configuration de Trusted Remediator
- Trusted Advisor Consulter le rapport récapitulatif

Rapport récapitulatif de Trusted Remediator Remediation

Le rapport Trusted Remediation Status fournit des informations sur les mesures correctives effectuées au cours des cycles de correction précédents. Le nombre de semaines par défaut est 1.

Pour personnaliser le rapport, spécifiez le nombre de semaines en fonction de votre calendrier de correction.

Nom du champ	Définition
Date	Date à laquelle les données ont été collectées.
ID de compte	L'ID du AWS compte auquel appartient la ressource
Nom du compte	Le nom du AWS compte
Vérifiez la catégorie	La catégorie de AWS Trusted Advisor chèques
Nom du chèque	Le nom de la vérification corrigée Trusted Advisor
ID de la vérification	L'ID du chèque corrigé Trusted Advisor
Mode d'exécution	Le mode d'exécution configuré pour le Trusted Advisor contrôle spécifique
OpsItem ID	L'ID du OpsItem créé par Trusted Advisor pour la correction
OpsItem État	Le statut du OpsItem créé par Trusted Advisor au moment de la création du rapport
ID de ressource	L'ARN de la ressource créée pour la correction

Rapport récapitulatif de configuration de Trusted Remediator

Le rapport récapitulatif de la configuration de Trusted Remediator fournit des informations sur les configurations actuelles de Trusted Remediator Remediation pour chaque vérification. Trusted Advisor

Nom du champ	Définition
Date	Date à laquelle les données ont été collectées.

Nom du champ	Définition
ID de compte	L'ID de AWS compte auquel s'applique la configuration
Nom du compte	Le nom du AWS compte
Vérifiez la catégorie	La catégorie de AWS Trusted Advisor chèques
Nom du chèque	Nom de la Trusted Advisor vérification corrigée à laquelle s'applique la configuration
ID de la vérification	L'ID du Trusted Advisor contrôle corrigé auquel s'applique la configuration
Mode d'exécution	Le mode d'exécution configuré pour le Trusted Advisor contrôle spécifique
Passer au mode automatique	Le modèle de balise, s'il est configuré, pour remplacer le mode d'exécution par Automatisé
Passer au mode manuel	Le modèle de balise, s'il est configuré, pour remplacer le mode d'exécution par Manuel

Trusted Advisor Consulter le rapport récapitulatif

Le rapport récapitulatif des Trusted Advisor vérifications fournit des informations sur les Trusted Advisor vérifications en cours. Ce rapport collecte des données après chaque programme de correction hebdomadaire. Le nombre de semaines par défaut est 1. Pour personnaliser le rapport, spécifiez le nombre de semaines en fonction de votre cycle de correction.

Nom du champ	Définition
Date	Date à laquelle les données ont été collectées.
ID de compte	L'ID de AWS compte auquel s'applique la configuration
Nom du client	Le nom du AWS compte

Nom du champ	Définition
Vérifiez la catégorie	La catégorie de AWS Trusted Advisor chèques
Nom du chèque	Nom de la Trusted Advisor vérification corrigée à laquelle s'applique la configuration
ID de la vérification	L'ID du Trusted Advisor contrôle corrigé auquel s'applique la configuration
Status	État d'alerte du contrôle. Les statuts possibles sont ok (vert), warning (jaune), error (rouge) ou not_available
Ressources signalées	Le nombre de AWS ressources signalées (répertoriées) par le Trusted Advisor chèque.
Ressources ignorées	Le nombre de AWS ressources qui ont été ignorées Trusted Advisor parce que vous les avez marquées comme supprimées.
Ressources dans un état critique	Le nombre de ressources dans un état critique
Ressources en état d'alerte	Nombre de ressources en état d'alerte

Rapports en libre-service

Les rapports en libre-service (SSR) d'AWS Managed Services (AMS) sont une fonctionnalité qui collecte des données à partir de divers AWS services natifs et donne accès aux rapports sur les principales offres AMS. Le SSR fournit des informations que vous pouvez utiliser pour soutenir les opérations, la gestion des configurations, la gestion des actifs, la gestion de la sécurité et la conformité.

Utilisez SSR pour accéder aux rapports depuis la console AMS et aux ensembles de données de rapports via des compartiments Amazon S3 (un compartiment par compte). Vous pouvez intégrer les données à votre outil de business intelligence (BI) préféré pour personnaliser les rapports en fonction de vos besoins uniques. AMS crée ce compartiment S3 (nom du compartiment S3 : (ams-reporting-

data-a<Account_ID>) dans votre AWS région principale, et les données sont partagées depuis le plan de contrôle AMS hébergé dans la région us-east-1.

Pour permettre à vos utilisateurs de consulter les rapports AMS Accelerate dans la console AMS, vous devez accorder des autorisations explicites dans AWS Identity and Access Management (IAM) pour effectuer ces actions. Par exemple, les politiques IAM, voir Autorisations d'utilisation des fonctionnalités AMS.

> **Important**
>
> Utilisation de clés personnalisées avec AWS Glue
> Pour chiffrer vos AWS Glue métadonnées à l'aide d'une clé KMS gérée par le client, vous devez effectuer les étapes supplémentaires suivantes pour permettre à AMS d'agréger les données du compte :
>
> 1. Ouvrez la AWS Key Management Service console à l'adresse https://console.aws.amazon.com/kms, puis choisissez Customer Managed Keys.
> 2. Sélectionnez l'ID de clé que vous comptez utiliser pour chiffrer les AWS Glue métadonnées.
> 3. Choisissez l'onglet Alias, puis sélectionnez Créer un alias.
> 4. Dans la zone de texte, entrez AmsReportingFlywheelCustomKey, puis choisissez Créer un alias.

Rubriques

- Opérations internes de l'API
- Rapport de patch (quotidien)
- Rapport de sauvegarde (quotidien)
- Rapport d'incident (hebdomadaire)
- Rapport de facturation (mensuel)
- Rapports agrégés
- Tableaux de bord de rapports en libre-service AMS
- Stratégie de conservation des données
- Débarquer de la SSR

Opérations internes de l'API

Si vous surveillez les opérations d'API, vous pouvez voir des appels aux opérations internes suivantes uniquement :

- `GetDashboardUrl`
- `ListReportsV2`

Fonctionnement interne de l'API : GetDashboardUrl

Cette opération apparaît dans les journaux système lorsqu'elle est invoquée par la console AMS. Il n'a aucun autre cas d'utilisation. Il n'est pas disponible pour votre usage direct.

Renvoie l'URL du tableau de bord intégré pour le rapport correspondant. Cette opération accepte un `dashboardName` retour par`ListReports`.

Syntaxe de demande

```
HTTP/1.1 200
Content-type: application/json
{
    "dashboardName": "string"
}
```

Éléments de la demande

`dashboardName`: nom du QuickSight tableau de bord pour lequel l'URL est demandée. Le nom du tableau de bord est renvoyé dans la ListReports version 2.

Type : String

Syntaxe de réponse

```
HTTP/1.1 200
Content-type: application/json
{
  "url": "string"
}
```

Éléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200. Les données suivantes sont renvoyées au format JSON par le service.

`url`: renvoie l' QuickSight URL de la demande`dashboardName`.

Type : String

Erreurs

Pour plus d'informations sur les erreurs communes à toutes les actions, consultez la section Erreurs courantes.

`BadRequestException`:

La demande soumise n'est pas valide. Par exemple, si la saisie est incomplète ou incorrecte. Consultez le message d'erreur qui l'accompagne pour plus de détails.

Code d’état HTTP : 400

`NotFoundException`:

La ressource demandée est introuvable. Assurez-vous que l'URI de la demande est correct.

Code d’état HTTP : 404

`TooManyRequestsException`:

La demande a atteint sa limite de limitation. Réessayez après la période spécifiée.

Code d’état HTTP : 429

`UnauthorizedException`:

La demande est refusée car l'appelant ne dispose pas des autorisations suffisantes.

Code d'état HTTP : 401

Fonctionnement interne de l'API : ListReports V2

Cette API apparaît dans les journaux système lorsqu'elle est invoquée par la console AMS. Il n'a aucun autre cas d'utilisation. Il n'est pas disponible pour votre usage direct.

Renvoie la liste des rapports opérationnels disponibles pour un compte donné.

Syntaxe de demande

La demande n'a pas de corps de demande.

Syntaxe de réponse

```
HTTP/1.1 200
Content-type: application/json
{
  "reportsList": [
    {
        "dashboard": "string",
        "lastUpdatedTime": "string",
    }
  ],
  "reportsType": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200. Les données suivantes sont renvoyées au format JSON par le service.

`reportsList`: liste des rapports opérationnels disponibles.

Type : Tableau d'objets du tableau de bord

`reportsType`: indique si un rapport est agrégé sur plusieurs comptes ou non.

Type : String

Erreurs

Pour plus d'informations sur les erreurs communes à toutes les actions, consultez la section Erreurs courantes.

`BadRequestException`:

La demande soumise n'est pas valide. Par exemple, la saisie est incomplète ou incorrecte. Consultez le message d'erreur qui l'accompagne pour plus de détails.

Code d'état HTTP : 400

`NotFoundException`:

La ressource demandée est introuvable. Assurez-vous que l'URI de la demande est correct.

Code d’état HTTP : 404

`TooManyRequestsException`:

La demande a atteint sa limite de limitation. Réessayez après la période spécifiée.

Code d’état HTTP : 429

`UnauthorizedException`:

La demande est refusée car l'appelant ne dispose pas des autorisations suffisantes.

Code d'état HTTP : 401

Rapport de patch (quotidien)

Rapports disponibles

- Résumé des détails de l'instance pour l'application de correctifs AMS
- Détails du patch
- Instances n'ayant pas reçu de correctifs

Résumé des détails de l'instance pour l'application de correctifs AMS

Il s'agit d'un rapport informatif qui permet d'identifier toutes les instances intégrées à AMS Patching, l'état du compte, les détails des instances, la couverture de la fenêtre de maintenance, le temps d'exécution de la fenêtre de maintenance, les détails de la pile et le type de plateforme.

Ce jeu de données fournit :

- Données relatives aux instances de production et de non-production d'un compte. Les étapes de production et de non-production sont dérivées du nom du compte et non des balises d'instance.
- Données sur la distribution des instances par type de plateforme. Le type de plateforme « N/A » apparaît lorsque AWS Systems Manager (SSM) ne parvient pas à obtenir les informations relatives à la plate-forme.
- Données sur la distribution de l'état des instances, le nombre d'instances en cours d'exécution, arrêtées ou en cours d'arrêt.

Nom du champ de console	Nom du champ du jeu de données	Définition
Restrictions d'accès	restriction_d'accès	Régions auxquelles l'accès est restreint
Identifiant du compte	aws_account_id	AWS ID de compte auquel appartient l'ID d'instance
ID du compte administrateur	aws_admin_account_id	AWS Organizations Compte de confiance que vous avez activé.
Nom du compte	account_name	AWS nom du compte
État du compte	état_du compte	État du compte AMS
	compte_SLA	Engagement en matière de service de compte AMS
Type de compte	malz_role	Rôle MALZ
Nom du groupe Auto Scaling	instance_asg_name	Nom du groupe Auto Scaling (ASG) qui contient l'instance
Identifiant de l'instance	instance_id	ID de l' EC2 instance
Nom de l'instance	nom_instance	Nom de l' EC2 instance
Groupe de correctifs d'instanc e	instance_patch_group	Nom du groupe de correctif s utilisé pour regrouper les instances et appliquer la même fenêtre de maintenance
Type de groupe de correctifs d'instance	type_group_patch_instance	Type de groupe de correctifs
Type de plate-forme d'instance	type_plateforme d'instance	Type de système d'exploitation (OS)

Nom du champ de console	Nom du champ du jeu de données	Définition
Nom de la plate-forme d'instance	nom_plateforme de l'instance	Nom du système d'exploitation (OS)
État de l'instance	instance_state	État au cours du cycle de vie de l' EC2 instance
Balises d'instance	ec2_tags	Les balises associées à l'ID d' EC2 instance Amazon
Zone d'atterrissage	drapeau malz_	Drapeau pour un compte lié à Malz
Couverture des fenêtres de maintenance	mw_covered_flag	Si une instance possède au moins une fenêtre de maintenance activée avec une date d'exécution future, elle est considérée comme couverte, sinon non couverte
Date/heure d'exécution de la fenêtre de maintenance	date_window_execution_time	La prochaine fois que la fenêtre de maintenance devrait s'exécuter
Date/heure d'exécution de la fenêtre de maintenance	date_window_execution_time	La prochaine fois que la fenêtre de maintenance devrait s'exécuter
Compte de production	compte prod_	Identifiant des comptes AMS prod, non-prod, selon que le nom du compte inclut ou non les valeurs « PROD » ou « NONPROD ».
Date/heure du rapport	jeu de données_date/heure	Date et heure de génération du rapport.

Nom du champ de console	Nom du champ du jeu de données	Définition
Nom de la pile	nom_stack_instance	Nom de la pile contenant l'instance
Type de pile	instance_stack_type	Stack AMS (infrastructure AMS intégrée au compte client) ou stack client (infrastructure gérée par AMS qui prend en charge les applications des clients)

Détails du patch

Ce rapport fournit des informations détaillées sur les correctifs et couvre les fenêtres de maintenance des différentes instances.

Ce rapport fournit :

- Données sur les groupes de correctifs et leurs types.
- Données sur les fenêtres de maintenance, leur durée, leur date limite, les dates futures d'exécution des fenêtres de maintenance (calendrier) et les instances concernées par chaque fenêtre.
- Données relatives à tous les systèmes d'exploitation associés au compte et nombre d'instances dans lesquelles le système d'exploitation est installé.

Nom du champ	Nom du champ du jeu de données	Définition
Date/heure du rapport	jeu de données_date/heure	Date et heure de génération du rapport.
Identifiant du compte	aws_account_id	AWS ID de compte auquel appartient l'ID d'instance
Nom du compte	account_name	AWS nom du compte

Nom du champ	Nom du champ du jeu de données	Définition
État du compte	état_du compte	État du compte AMS
Conforme - Critique	compliant_critique	Nombre de correctifs conformes présentant un niveau de gravité « critique »
Conforme - Élevé	compliant_high	Nombre de correctifs conformes présentant un niveau de gravité « élevé »
Conforme - Moyen	compliant_medium	Nombre de correctifs conformes de gravité « moyenne »
Conforme - Faible	compliant_faible	Nombre de correctifs conformes dont le niveau de gravité est « faible »
Conforme - Informatif	compliant_informational	Nombre de correctifs conformes dont le niveau de gravité est « informatif »
Conforme - Non spécifié	compliant_non spécifié	Nombre de correctifs conformes dont le niveau de gravité est « non spécifié »
Conforme - Total	total_conforme	Nombre de correctifs conformes (tous niveaux de gravité confondus)
Identifiant de l'instance	instance_id	ID de l' EC2 instance
Nom de l'instance	nom_instance	Nom de l' EC2 instance
	compte_SLA	Niveau de service du compte AMS

Nom du champ	Nom du champ du jeu de données	Définition
Type de plate-forme d'instance	type_plateforme d'instance	Type de système d'exploitation (OS)
Nom de la plate-forme d'instance	nom_plateforme de l'instance	Nom du système d'exploitation (OS)
Type de groupe de correctifs d'instance	type_group_patch_instance	PAR DÉFAUT : groupe de correctifs par défaut avec fenêtre de maintenance par défaut, déterminé par la AMSDefault PatchGroup balise :TRUE sur l'instance CLIENT : groupe de correctifs créé par le client NOT_ASSIGNED : aucun groupe de correctifs n'est attribué
Groupe de correctifs d'instance	instance_patch_group	Nom du groupe de correctifs utilisé pour regrouper les instances et appliquer la même fenêtre de maintenance
État de l'instance	instance_state	État dans le cycle de vie de l'EC2 instance
Balises d'instance	ec2_tags	Les balises associées à l'ID d'EC2 instance Amazon
Fenêtre de maintenance de la dernière exécution	dernière_fenêtre_d'exécution	Dernière exécution de la fenêtre de maintenance
ID de fenêtre de maintenance	identifiant de fenêtre	ID de la fenêtre de maintenance

Nom du champ	Nom du champ du jeu de données	Définition
État de la fenêtre de maintenance	état_fenêtre	État de la fenêtre de maintenance
Type de fenêtre de maintenance	type_fenêtre	Type de fenêtre de maintenance
Date et heure de la prochaine exécution de la fenêtre de maintenance	fenêtre_suivante execution_time	La prochaine fois que la fenêtre de maintenance devrait s'exécuter
Durée de la fenêtre de maintenance (heures)	durée_fenêtre	Durée de la fenêtre de maintenance en heures
Couverture des fenêtres de maintenance	mw_covered_flag	Si une instance possède au moins une fenêtre de maintenance activée avec une date d'exécution future, elle est considérée comme couverte, sinon non couverte
Non conforme - Critique	non conformité_critique	Nombre de correctifs non conformes présentant une gravité « critique »
Non conforme - Élevé	non conformit_high	Nombre de correctifs non conformes présentant un niveau de gravité « élevé »
Non conforme - Moyen	médium_non conforme	Nombre de correctifs non conformes de gravité « moyenne »
Non conforme - Faible	non conformit_faible	Nombre de correctifs non conformes dont le niveau de gravité est « faible »

Nom du champ	Nom du champ du jeu de données	Définition
Non conforme - Informatif	non conforme _informatif	Nombre de correctifs non conformes dont le niveau de gravité est « informatif »
Non conforme - Non spécifié	non conforme _non spécifié	Nombre de correctifs non conformes dont la gravité est « non spécifiée »
Non conforme - Total	total_non conforme	Nombre de correctifs non conformes (tous niveaux de gravité confondus)
ID de référence du correctif	patch_baseline_id	Ligne de base de correctif s actuellement attachée à l'instance
État du correctif	état_du correctif	État général de conformité des correctifs. S'il manque au moins un correctif, l'instanc e est considérée comme non conforme, sinon conforme.
Compte de production	compte prod_	Identifiant des comptes AMS prod, non-prod, selon que le nom du compte inclut ou non les valeurs « PROD » ou « NONPROD ».
Type de pile	instance_stack_type	Stack AMS (infrastructure AMS intégrée au compte client) ou stack client (infrastr ucture gérée par AMS qui prend en charge les applicati ons des clients)

Nom du champ	Nom du champ du jeu de données	Définition
	window_next_exec_yyyy	Année comprise dans window_next_execution_time
	window_next_exec_mm	Partie mensuelle de window_next_execution_time
	Window_Next_Exec_D	Partie journalière de window_next_execution_time
	fenêtre_suivante _Exec_HHMI	Heure : partie minute de window_next_execution_time

Instances n'ayant pas reçu de correctifs

Ce rapport fournit des informations détaillées sur les instances pour lesquelles des correctifs n'ont pas été corrigés lors de la dernière exécution de la fenêtre de maintenance.

Ce rapport fournit :

- Données sur les correctifs manquants au niveau de l'ID du correctif.
- Des données sur toutes les instances pour lesquelles au moins un correctif est manquant et des attributs tels que la gravité du correctif, le nombre de jours sans correctif, la plage et la date de sortie du correctif.

Nom du champ	Nom du champ du jeu de données	Définition
Date/heure du rapport	jeu de données_date/heure	Date et heure de génération du rapport
Identifiant du compte	aws_account_id	AWS ID de compte auquel appartient l'ID d'instance
Nom du compte	account_name	AWS nom du compte

Nom du champ	Nom du champ du jeu de données	Définition
Nom du client Parent	nom_client_parent	
Nom du client	nom_client	
Compte de production	compte prod_	Identifiant des comptes AMS prod ou non, selon que le nom du compte inclut la valeur « PROD » ou « NONPROD ».
État du compte	état_du compte	État du compte AMS
Type de compte	type_compte	
	compte_SLA	Niveau de service du compte AMS
Identifiant de l'instance	instance_id	ID de votre EC2 instance
Nom de l'instance	nom_instance	Nom de votre EC2 instance
Type de plate-forme d'instance	type_plateforme d'instance	Type de système d'exploitation (OS)
État de l'instance	instance_state	État dans le cycle de vie de l' EC2 instance
Balises d'instance	ec2_tags	Les balises associées à l'ID d' EC2 instance Amazon
Identifiant du correctif	ID du correctif	ID du correctif publié
Gravité des correctifs	patch_sev	Gravité du correctif par éditeur
Classification des correctifs	patch_class	Classification des correctifs selon l'éditeur du correctif

Nom du champ	Nom du champ du jeu de données	Définition
Date de publication du correctif (UTC)	release_dt_utc	Date de sortie du correctif par éditeur
État d'installation du correctif	état_d'installation	État d'installation du correctif sur une instance par SSM
Jours non corrigés	days_unpatched	Nombre de jours pendant lesquels l'instance n'a pas reçu de correctif depuis le dernier scan SSM
Nombre de jours non patchés	days_unpatched_bucket	Nombre de jours non corrigés

Rapport de sauvegarde (quotidien)

Le rapport de sauvegarde couvre les régions principales et secondaires (le cas échéant). Il couvre l'état des sauvegardes (succès/échec) et les données relatives aux instantanés pris.

Ce rapport fournit :

- État de la sauvegarde
- Nombre de clichés pris
- Point de récupération
- Plan de sauvegarde et informations sur le coffre-fort

Nom du champ	Nom du champ du jeu de données	Définition
Date/heure du rapport	jeu de données_date/heure	Date et heure de génération du rapport.
ID du compte	aws_account_id	ID de compte AWS auquel appartient l'ID d'instance

Nom du champ	Nom du champ du jeu de données	Définition
ID du compte administrateur	aws_admin_account_id	AWS Organizations Compte de confiance que vous avez activé.
Nom du compte	account_name	Nom du compte AWS
Compte SLA	compte_SLA	Engagement en matière de service de compte AMS
	drapeau malz_	Drapeau pour un compte lié à Malz
	malz_role	Rôle MALZ
	restriction_d'accès	Régions auxquelles l'accès est restreint
Backup : date/heure de début planifiée	start_by_dt_utc	Horodatage auquel le début de la capture d'écran est prévu
Backup, capture instantanée, date de début réelle	creation_dt_utc	Horodatage du début réel de l'instantané
Backup : date/heure d'achèvement du snapshot	complétion_dt_utc	Horodatage lorsque le cliché est terminé
Backup : date/heure d'expiration du snapshot	expiration_dt_utc	Horodatage à l'expiration de l'instantané
État du Backup Job	backup_job_status	État de l'instantané
Type de sauvegarde	type_de sauvegarde	Type de sauvegarde
ID de la tâche de sauvegarde	backup_job_id	Identifiant unique de la tâche de sauvegarde

Nom du champ	Nom du champ du jeu de données	Définition
Taille de sauvegarde en octets	taille_de_sauvegarde en octets	Taille de sauvegarde en octets
Plan de sauvegarde (ARN)	backup_plan_arn	L'ARN du plan de sauvegarde
ID du plan de sauvegarde	ID du plan_sauvegarde	Identifiant unique du plan de sauvegarde
Nom du plan de sauvegarde	nom_plan_de sauvegarde	Le nom du plan de sauvegard e
Version du plan de sauvegard e	version du plan de sauvegarde	Version du plan de sauvegard e
ID de règle de sauvegarde	ID de rule_sauvegarde	L'identifiant de la règle de sauvegarde
Backup Vault (ARN)	backup_vault_arn	Backup Vault (ARN)
Nom du coffre-fort de sauvegarde	nom_coffre de sauvegarde	Le nom du coffre de sauvegarde
ARN du rôle IAM	iam_role_arn	L'ARN du rôle IAM
Identifiant de l'instance	instance_id	ID d'instance unique
État de l'instance	instance_state	État de l’instance
Balises d'instance	ec2_tags	Les balises associées à l'ID d' EC2 instance
ARN des ressources	resource_arn	Le nom de la ressource Amazon
ID de ressource	identifiant_ressource	L'identifiant de ressource unique

Nom du champ	Nom du champ du jeu de données	Définition
Région de ressources	région_ressource	Les régions principales (et secondaires, le cas échéant) de la ressource.
Type de ressource	type_ressource	Le type de ressource
Point de récupération (ARN)	recovery_point_arn	L'ARN du point de récupérat ion
Identifiant du point de récupération	identifiant_point de récupérat ion	L'identifiant unique du point de récupération
État du point de restauration	État du point de récupération	Statut du point de récupération
Suppression du point de restauration après plusieurs jours	recovery_point_delete_after _days	Suppression du point de récupération après plusieurs jours
Le point de récupération est transféré dans une chambre froide après plusieurs jours	recovery_point_move_to_cold _storage_after_days	Nombre de jours après la date d'achèvement pendant lesquels l'instantané de sauvegarde est transféré vers un stockage à froid
État du chiffrement du point de restauration	le point de récupération est crypté	État du chiffrement du point de restauration
ARN de la clé de chiffrement Recovery Point	recovery_point_encryption_k ey_arn	ARN de la clé de chiffrement du point de récupération
ID de pile	stack_id	Identifiant unique de la pile Cloudformation
Nom de la pile	stack_name	Nom de la pile

Nom du champ	Nom du champ du jeu de données	Définition
Tag : Groupe de correctifs par défaut AMS	tag_ams_default_patch_group	Valeur de balise : groupe de correctifs par défaut AMS
Tag : App Id	tag_app_id	Valeur du tag : App ID
Tag : Nom de l'application	nom_app_tag	Valeur du tag : nom de l'application
Tag : Backup	tag_backup	Valeur du tag : Backup
Tag : Cadre de conformité	tag_compliance_framework	Valeur du tag : Cadre de conformité
Tag : Centre de coûts	tag_cost_center	Valeur du tag : Cost Center
Tag : Client	tag_client	Valeur du tag : Client
Tag : Classification des données	tag_data_classification	Valeur du tag : classification des données
Tag : Type d'environnement	tag_environnement_type	Valeur du tag : Type d'environnement
Tag : Heures d'ouverture	tag_heures_of_operation	Valeur du tag : Heures d'ouverture
Tag : Équipe propriétaire	tag_owner_team	Valeur du tag : Owner Team
Tag : Email de l'équipe du propriétaire	tag_owner_team_email	Valeur du tag : e-mail de l'équipe du propriétaire
Tag : Patch Group	tag_patch_group	Valeur du tag : Patch Group
Tag : Support Priority	tag_support_priority	Valeur du tag : Support Priority
État du volume	état_volume	État du volume

Rapport d'incident (hebdomadaire)

Ce rapport fournit la liste agrégée des incidents ainsi que leur priorité, leur gravité et leur état le plus récent, notamment :

- Données sur les cas de support classés comme des incidents sur le compte géré
- Informations sur les incidents requises pour visualiser les mesures relatives aux incidents pour le compte géré
- Données sur les catégories d'incidents et l'état des mesures correctives pour chaque incident

La visualisation et les données sont disponibles pour le rapport d'incident hebdomadaire.

- La visualisation est accessible via la console AMS du compte via la page Rapports.
- Le jeu de données avec le schéma suivant est accessible via le compartiment S3 du compte géré.
- Utilisez les champs de date fournis pour filtrer les incidents en fonction du mois, du trimestre, de la semaine ou du and/or jour où l'incident a été créé ou résolu.

Nom du champ	Nom du champ du jeu de données	Définition
Date/heure du rapport	jeu de données_date/heure	Date et heure de génération du rapport.
Identifiant du compte	aws_account_id	AWS ID du compte auquel appartient l'incident.
ID du compte administrateur	aws_admin_account_id	AWS Organizations Compte de confiance que vous avez activé.
Nom du compte	account_name	AWS nom du compte.
Numéro du dossier	case_id	L'identifiant de l'incident.
Mois de création	mois_créé	Le mois où l'incident a été créé.

Nom du champ	Nom du champ du jeu de données	Définition
Priority (Priorité)	priority	Priorité de l'incident.
Sévérité	severity	La gravité de l'incident.
Status	status	État de l'incident.
Catégorie	catégorie_yuma	Catégorie de l'incident.
Jour de création	jour_créé	Le jour où l'incident a été créé au YYYY-MM-DD format.
Semaine de création	created_wk	Semaine au cours de laquelle l'incident a été créé au format YYYY-WW. Le dimanche et le samedi sont comptés comme le début et la fin d'une semaine. La semaine va de 01 à 52. La semaine 01 est toujours la semaine qui contient le premier jour de l'année. Par exemple, les 31 décembre 2023 et 01/2024 correspondent à la semaine 2024-01.
Trimestre créé	created_qtr	Le trimestre au cours duquel l'incident a été créé au format YYYY-Q. Le 01/01 au 31/03 est défini comme Q1, etc.
Jour résolu	jour_résolu	Le jour où l'incident a été résolu dans le YYYY-MM-DD format.

Nom du champ	Nom du champ du jeu de données	Définition
Semaine résolue	resolved_wk	Semaine au cours de laquelle l'incident a été résolu au format YYYY-WW. Le dimanche et le samedi sont comptés comme le début et la fin d'une semaine. La semaine va de 01 à 52. La semaine 01 est toujours la semaine qui contient le premier jour de l'année. Par exemple, les 31 décembre 2023 et 01/2024 correspondent à la semaine 2024-01.
Mois résolu	mois_résolu	Le mois où l'incident a été résolu au format YYYY-MM.
Trimestre résolu	resolved_qtr	Le trimestre au cours duquel l'incident a été résolu au format YYYY-Q. Le 01/01 au 31/03 est défini comme Q1, etc.
Règle de regroupement créée	regle_de regroupement	Règle de regroupement qui s'applique à l'inciden t. « no_grouping » ou « instance_grouping ».
Instance IDs	identifiants d'instance	Instance associée à l'incident.

Nom du champ	Nom du champ du jeu de données	Définition
Nombre d'alertes	nombre_d'alertes	Le nombre d'alertes associées à cet incident. Si le regroupement est activé, ce nombre peut être supérieur à 1. Si le regroupement n'est pas activé, il sera toujours égal à 1.
Création à	created_at	Horodatage de la création de l'incident.
Alarme ARNs	alarm_arns	Le nom de ressource Amazon (« arn ») des alarmes associées à votre incident.
Alarmes associées	alarmes associées	Les noms lisibles par l'homme de toutes les alarmes associées à l'incident.

Rapport de facturation (mensuel)

Détails des frais de facturation

Ce rapport fournit des informations détaillées sur les frais de facturation d'AMS avec les comptes associés et les services AWS correspondants.

Ce rapport fournit :

- Données sur les frais de niveau de service AMS, les pourcentages d'augmentation, les niveaux de service AMS au niveau du compte et les frais AMS.
- Données sur les comptes associés et les frais d'utilisation d'AWS.

> **Important**
>
> Le rapport de facturation mensuel est uniquement disponible sur votre compte de payeur de gestion (MPA) ou sur votre compte débité défini. Il s'agit des comptes sur lesquels votre facture mensuelle AMS est envoyée. Si vous ne parvenez pas à localiser ces comptes, contactez votre responsable de prestation de services cloud (CSDM) pour obtenir de l'aide.

Nom du champ	Nom du champ du jeu de données	Définition
Date de facturation	date	Le mois et l'année du service facturé
Identifiant du compte du payeur	ID de compte_payeur	L'identifiant à 12 chiffres identifiant le compte responsable du paiement des frais AMS
Identifiant du compte associé	identifiant_compte_lié	L'identifiant à 12 chiffres identifiant le compte AMS qui consomme des services et génère des étendues
AWS Nom du service	product_name	Le AWS service qui a été utilisé
AWS Charges	taxes_frais	Les AWS frais associés au nom du AWS service dans Nom du AWS service
Plan de tarification	plan de tarification	Le plan tarifaire associé au compte associé
Groupe de services AMS	tier_uplifting_groups	Code de groupe de services AMS qui détermine le pourcentage d'élévation

Nom du champ	Nom du champ du jeu de données	Définition
Proportion de levage	uplift_percent	Le pourcentage d'augment ation (sous forme décimale V.WXYZ) basé sur pricing_p lan, SLA et service AWS
AWS Charges ajustées	utilisation_aws_ajustable	AWS utilisation ajustée pour AMS
Charges augmentées AWS	factures_majorées_facturati ons	Pourcentage de AWS frais à facturer pour AMS ; adjust_aw s_charges * uplift_percent
Instances : EC2 dépenses RDS	instances_ec2_rds_spend	Dépenses consacrées EC2 aux instances RDS
Frais relatifs aux instances réservées	ris_charges	Frais relatifs aux instances réservées
Frais d'instance réservés augmentés	uplifted_ris	Pourcentage des frais d'instance réservée à facturer pour AMS ; ris_charges * uplift_percent
Frais du Savings Plan	sp_charges	SavingsPlan frais d'utilisation
Frais majorés du Savings Plan	uplifted_sp	Le pourcentage des frais des plans d'épargne à facturer pour AMS ; sp_charges * uplift_percent
Frais AMS	ams_charges	Total des frais d'armes pour le produit ; uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp

Nom du champ	Nom du champ du jeu de données	Définition
Frais minimaux calculés au prorata	minimal_calculé au prorata	Le montant que nous facturons pour respecter le minimum contractuel
Total des frais AMS du compte lié	total du compte lié ams_charges	Somme de tous les frais pour le link_account
Total des frais AMS du compte du payeur	total du compte payeur ams_charges	Somme de tous les frais pour le compte du payeur
Frais minimaux	frais_minimums	Frais minimaux d'AMS (le cas échéant)
Réduction sur les instances réservées et le Savings Plan	adj_ri_sp_charges	RI/SP discount to be applied against RI/SPfrais (applicables dans certaines circonstances)

Rapports agrégés

Les rapports agrégés en libre-service (SSR) vous fournissent une vue des rapports en libre-service existants agrégés au niveau de l'organisation, entre comptes. Cela vous donne une visibilité sur les indicateurs opérationnels clés, tels que la conformité des correctifs, la couverture des sauvegardes et les incidents, sur tous les comptes gérés par AMS au sein de votre entreprise AWS Organizations.

Le SSR agrégé est disponible dans toutes les entreprises Régions AWS où AWS Managed Services est disponible. Pour une liste complète des régions disponibles, consultez le tableau des régions.

Activer les rapports agrégés

Vous devez gérer le SSR agrégé à partir d'un compte AWS Organizations de gestion. Le compte de gestion est le AWS compte que vous avez utilisé pour créer votre organisation.

Pour activer le SSR agrégé pour un compte de AWS Organizations gestion intégré à AMS, accédez à votre console AMS et accédez à Reports. Sélectionnez Organization Access dans le top-right-hand

coin pour ouvrir le volet AWS Managed Services Console : Organization View. Dans ce volet, vous pouvez gérer la fonctionnalité SSR agrégée.

AWS Organizations les comptes de gestion qui ne sont pas intégrés à AMS n'ont pas accès à la console AMS. Pour activer le SSR agrégé pour un compte AWS Organizations de gestion qui n'est pas intégré à AMS, authentifiez-vous d'abord auprès de votre compte Compte AWS, puis accédez à la AWS console et recherchez Managed Services. Cela ouvre la page AMS Marketing. Sur cette page, sélectionnez le lien Organization Access dans la barre de navigation pour ouvrir la console AWS Managed Services : Organization View, dans laquelle vous pouvez gérer la fonctionnalité Aggregated SSR.

La première fois que vous accédez à la console AWS Managed Services : Organization View, procédez comme suit :

1. Si ce n'est pas déjà fait AWS Organizations, choisissez Activer AWS Organizations sur votre console. Pour plus d'informations sur la configuration AWS Organizations, consultez le guide de AWS Organizations l'utilisateur. Vous pouvez ignorer cette étape si vous l'utilisez déjà AWS Organizations.
2. Pour activer le service de rapports agrégés en libre-service, sélectionnez Activer l'accès sécurisé sur la console.
3. (Facultatif) Enregistrez un administrateur délégué pour bénéficier d'un accès en lecture à la vue organisationnelle.

Afficher les rapports agrégés en tant qu'administrateur délégué

Un administrateur délégué est le compte que vous choisissez pour avoir accès en lecture aux rapports agrégés. L'administrateur délégué doit être un compte intégré à AMS et être le seul à avoir un accès en lecture aux rapports agrégés.

Pour choisir un administrateur délégué, entrez l'ID du compte à l'étape 3 sur la console AWS Managed Services : Organization View. Vous ne pouvez avoir qu'un seul compte d'administrateur délégué enregistré à la fois. Notez que le compte d'administrateur délégué doit être un compte géré par AMS.

Pour mettre à jour un compte d'administrateur délégué, accédez à la console AWS Managed Services : Organization View et sélectionnez Supprimer l'administrateur délégué. La console vous invite à saisir un nouvel identifiant de compte pour vous enregistrer en tant qu'administrateur délégué.

Lire des rapports agrégés

Si vous n'enregistrez pas d'administrateur délégué et que votre compte de AWS Organizations gestion est intégré à AMS, le compte de AWS Organizations gestion obtient un accès en lecture aux rapports agrégés par défaut. Si le compte AWS Organizations de gestion n'est pas géré par AMS, vous devez choisir un compte d'administrateur délégué pour avoir un accès en lecture aux rapports agrégés.

À tout moment, un seul compte intégré à AMS a accès en lecture aux rapports agrégés, qu'il s'agisse du compte de AWS Organizations gestion ou de l'administrateur délégué enregistré. Tous les autres comptes membres de votre organisation (et intégrés à AMS) n'ont toujours accès qu'aux rapports sur un seul compte pour chaque compte individuel.

Après avoir activé le SSR agrégé, accédez à vos rapports. Tous vos rapports en libre-service existants sont répertoriés dans cette section, et une balise bleue indique qu'ils ont été agrégés. Notez que vous devez accéder à la console AMS depuis le compte que vous avez choisi pour avoir un accès en lecture aux rapports agrégés. Il s'agit du compte AWS Organizations de gestion ou du compte d'administrateur délégué.

Une fois que vous avez activé le SSR agrégé, les rapports agrégés sont disponibles à partir du cycle de reporting suivant.

Désactiver les rapports agrégés

Pour désactiver le SSR agrégé, ouvrez la console AWS Managed Services : Organization View. Sélectionnez Désactiver l'accès sécurisé. Une fois que vous avez désactivé l'accès sécurisé pour le SSR agrégé, vos rapports en libre-service AMS cessent d'être agrégés au niveau de l'organisation, sur tous les comptes. Notez également que la désactivation prend effet à compter du prochain cycle de rapports.

Après avoir désactivé le SSR agrégé, vous devez attendre avant que les rapports de votre console AMS apparaissent sous forme de rapports à compte unique. Ce délai est dû au fait que la désactivation de la fonctionnalité prend effet à compter du cycle de reporting suivant.

Tableaux de bord de rapports en libre-service AMS

Les rapports en libre-service d'AMS proposent deux tableaux de bord : Tableau de bord Resource Tagger et. Tableau de bord des règles de configuration de sécurité

Tableau de bord Resource Tagger

Le tableau de bord AMS Resource Tagger fournit des informations détaillées sur les ressources prises en charge par Resource Tagger, ainsi que sur l'état actuel des balises que Resource Tagger est configuré pour appliquer à ces ressources.

Couverture du Resource Tagger par type de ressource

Cet ensemble de données consiste en une liste de ressources dont les balises sont gérées par Resource Tagger.

La couverture des ressources par type de ressource est visualisée sous la forme de quatre graphiques linéaires qui décrivent les mesures suivantes :

- Nombre de ressources : nombre total de ressources dans la région, par type de ressource.
- Ressources sans balises gérées : nombre total de ressources de la région, par type de ressource, qui nécessitent des balises gérées mais ne sont pas étiquetées par Resource Tagger.
- Ressources non gérées : nombre total de ressources de la région, par type de ressource, auxquelles aucune balise gérée n'a été appliquée par Resource Tagger. Cela signifie généralement que ces ressources ne correspondent à aucune configuration de Resource Tagger ou qu'elles sont explicitement exclues des configurations.
- Ressources gérées : équivalent à la métrique des ressources non gérées (nombre de ressources - Ressources non gérées).

Le tableau suivant répertorie les données fournies par ce rapport.

Nom de champ	Nom du champ du jeu de données	Définition
Date/heure du rapport	jeu de données_date/heure	Date et heure de génération du rapport (heure UTC)
Compte AWS ID	aws_account_id	Compte AWS ID
ID du compte administrateur	aws_admin_account_id	AWS Organizations Compte de confiance que vous avez activé.

Nom de champ	Nom du champ du jeu de données	Définition
Region (Région)	region	Région AWS
Type de ressource	type_ressource	Ce champ identifie le type de ressource. Seuls les types de ressources pris en charge par Resource Tagger sont inclus.
Nombre de ressources	nombre de ressources	Nombre de ressources (du type de ressource spécifié) déployées dans cette région.
ResourcesMissingManagedTags	resource_missing_managed_tags_count	Nombre de ressources (du type de ressource spécifié) qui nécessitent des balises gérées, selon les profils de configuration, mais qui n'ont pas encore été étiquetées par Resource Tagger.
UnmanagedResources	comptage de ressources_non géré	Nombre de ressources (du type de ressource spécifié) auxquelles aucune balise gérée n'est appliquée par Resource Tagger. Généralement, ces ressources ne correspondent à aucun bloc de configuration du Resource Tagger ou sont explicitement exclues des blocs de configuration.

Conformité aux règles de configuration du Resource Tagger

Cet ensemble de données consiste en une liste de ressources dans un Région AWS, par type de ressource, auxquelles un certain profil de configuration leur est appliqué. Il est visualisé sous la forme d'un graphique linéaire.

Le tableau suivant répertorie les données fournies par ce rapport.

Nom de champ	Nom du champ du jeu de données	Définition
Date/heure du rapport	jeu de données_date/heure	Date et heure de génération du rapport (heure UTC)
Compte AWS ID	aws_account_id	Compte AWS ID
ID du compte administrateur	aws_admin_account_id	AWS Organizations Compte de confiance que vous avez activé.
Region (Région)	region	Région AWS
Type de ressource	type_ressource	Ce champ identifie le type de ressource. Seuls les types de ressources pris en charge par Resource Tagger sont inclus.
ID du profil de configuration	identifiant_profil_configuration	ID du profil de configuration du Resource Tagger. Un profil de configuration est utilisé pour définir les politiques et les règles utilisées pour étiqueter vos ressources.
MatchingResourceCount	nombre de ressources	Nombre de ressource s (du type de ressource spécifié) correspondant à l'ID du profil de configuration Resource Tagger. Pour qu'une

Nom de champ	Nom du champ du jeu de données	Définition
		ressource corresponde au profil de configuration, le profil doit être activé et la ressource doit correspondre à la règle du profil.

Ressources non conformes à Resource Tagger

Cet ensemble de données consiste en une liste de ressources non conformes pour une seule configuration de Resource Tagger. Ces données constituent un instantané quotidien de la conformité des ressources, montrant l'état des ressources des clients au moment où ces rapports sont transmis aux comptes clients (il n'existe pas de vue historique). Il est visualisé sous la forme d'un tableau croisé dynamique composé de ressources non conformes à une configuration donnée.

Le tableau suivant répertorie les données fournies par ce rapport.

Nom de champ	Nom du champ du jeu de données	Définition
Date/heure du rapport	jeu de données_date/heure	Date et heure de génération du rapport (heure UTC)
Compte AWS ID	aws_account_id	Compte AWS ID
ID du compte administrateur	aws_admin_account_id	AWS Organizations Compte de confiance que vous avez activé.
Region (Région)	region	Région AWS
Type de ressource	type_ressource	Ce champ identifie le type de ressource. Seuls les types de ressources pris en charge par Resource Tagger sont inclus.

Nom de champ	Nom du champ du jeu de données	Définition
ID de ressource	identifiant_ressource	Identifiant unique des ressources prises en charge par Resource Tagger.
État de couverture	état_de couverture	Ce champ indique si la ressource est étiquetée comme configuré par l'ID de configuration du Resource Tagger.
ID du profil de configuration	identifiant_profil_configuration	ID du profil de configuration du Resource Tagger. Un profil de configuration est utilisé pour définir les politiques et les règles utilisées pour étiqueter vos ressources.

Tableau de bord des règles de configuration de sécurité

Le tableau de bord des règles de configuration de sécurité fournit un aperçu détaillé de la conformité des comptes AMS en termes de ressources et de AWS Config règles. Vous pouvez filtrer le rapport en fonction de la sévérité des règles afin de hiérarchiser les résultats les plus critiques. Le tableau suivant répertorie les données fournies par ce rapport.

Nom de champ	Nom du champ du jeu de données	Définition
Compte AWS ID	Compte AWS ID	L'identifiant du compte lié aux ressources associées.
ID du compte administrateur	aws_admin_account_id	AWS Organizations Compte de confiance que vous avez activé.

Nom de champ	Nom du champ du jeu de données	Définition
date/heure du rapport	Date du rapport	Date et heure de génération du rapport.
nom_client	Nom du client	Le nom du client.
account_name	Nom du compte	Le nom associé à l'identifiant du compte
identifiant_ressource	ID de ressource	Identifiant d'une ressource.
région_ressource	Région de ressources	L' Région AWS endroit où se trouve la ressource.
type_ressource	Type de ressource	Le type de ressource Service AWS or.
nom_ressource	Nom de la ressource	Le nom de la ressource.
resource_ams_flag	Drapeau AMS de ressources	Si la ressource appartien t à AMS, cet indicateur est défini sur TRUE. Si la ressource appartient au client, cet indicateur est défini sur FALSE. Si le propriétaire n'est pas connu, cet indicateur est défini sur UNKNOWN.
regle_configuration	Règle de configuration	Le nom non personnalisable de la règle de configuration.
description de la règle de configuration	Description de la règle de configuration	Description de la règle de configuration.

Nom de champ	Nom du champ du jeu de données	Définition
identifiant_source	Identifiant de source	Identifiant unique pour la règle de configuration gérée et aucun identifiant pour une règle de configuration personnalisée.
drapeau de conformité	Drapeau de conformité	Indique si les ressources sont conformes ou non aux règles de configuration.
type_règle	Type de règle	Indique si la règle est prédéfini e ou créée sur mesure.
drapeau d'exception	Drapeau d'exception	L'indicateur d'exception de ressource indique l'accepta tion du risque par rapport à une ressource non conforme. Si l'indicateur d'exception de ressource est VRAI pour une ressource, celle-ci est exemptée. Si l'indicateur d'exception est NULL, la ressource n'est pas exemptée.
cal_dt	Date	Date d'évaluation de la règle.
description_d'assainissement	Description de la remédiation	Description de la manière de remédier à la conformité aux règles.
severity	Sévérité	La sévérité de la règle de configuration indique l'impact de la non-conformité.

Nom de champ	Nom du champ du jeu de données	Définition
action_client	Action du client	Vous devez prendre les mesures nécessaires pour remédier à cette règle.
recommandation	Recommandation	Description de ce que la règle de configuration vérifie.
catégorie_remédiation	Catégorie de remédiation	Actions par défaut effectuée s par AMS lorsque cette règle devient non conforme.

Stratégie de conservation des données

AMS SSR applique une politique de conservation des données par rapport après la période indiquée, les données sont effacées et ne sont plus disponibles.

Nom du rapport	Console SSR de conservation des données	Bucket SSR S3 de conservat ion des données
Résumé des détails de l'instance pour l'application de correctifs AMS	2 mois	2 ans
Détails du patch	2 mois	2 ans
Instances n'ayant pas reçu de correctifs lors de l'exécution de la fenêtre de maintenance	2 mois	2 ans
Détails des frais de facturation AMS	2 ans	2 ans
Rapport de sauvegarde quotidien	1 mois	2 ans

Nom du rapport	Console SSR de conservation des données	Bucket SSR S3 de conservation des données
Rapport d'incident hebdomadaire	2 mois	2 ans
Tableau de bord des règles de configuration de sécurité	3 mois	2 ans
Tableau de bord Resource Tagger	1 an	2 ans

Débarquer de la SSR

Pour quitter le service SSR, créez une demande de service (SR) via la console AMS. Après avoir soumis le SR, un ingénieur des opérations AMS vous aide à quitter le SSR. Dans le SR, indiquez la raison pour laquelle vous souhaitez débarquer.

Pour déconnecter un compte et effectuer un nettoyage des ressources, créez un SR via la console AMS. Après avoir soumis le SR, un ingénieur des opérations AMS vous aide à supprimer le compartiment SSR Amazon S3.

Si vous quittez AMS, vous êtes automatiquement déconnecté de la console AMS SSR. AMS arrête automatiquement d'envoyer des données à votre compte. AMS supprime votre compartiment SSR S3 dans le cadre du processus d'offboarding.

Gestion des accès dans AMS Accelerate

La gestion des accès est la façon dont vos ressources sont protégées en n'autorisant que les accès autorisés et authentifiés. Avec AMS Accelerate, vous êtes responsable de la gestion de l'accès à vos ressources Comptes AWS et à leurs ressources sous-jacentes, telles que les solutions de gestion des accès, les politiques d'accès et les processus associés. Afin de vous aider à gérer votre solution d'accès, AMS Accelerate déploie des AWS Config règles qui détectent les erreurs de configuration courantes de l'IAM, puis fournissent des notifications de correction. Une erreur de configuration courante de l'IAM est que l'utilisateur root possède des clés d'accès. La règle de `iam-root-access-key-check` configuration vérifie si la clé d'accès de l'utilisateur root est disponible et est conforme ou si la clé d'accès n'existe pas. Pour obtenir la liste des règles de configuration déployées par AMS, consultez la bibliothèque de AWS Config règles AMS.

Rubriques

- Accédez à la console Accelerate
- Autorisations d'utilisation des fonctionnalités AMS
- Pourquoi et quand AMS accède à votre compte
- Comment AMS accède à votre compte
- Comment et quand utiliser le compte utilisateur root dans AMS

Accédez à la console Accelerate

Lorsque vous intégrez Accelerate, vous avez automatiquement accès à la console Accelerate. Vous pouvez accéder à la console en recherchant Managed Services dans votre console de gestion AWS. La console Accelerate vous donne une vue résumée des fonctionnalités dont vous disposez avec Accelerate. Cette vue inclut les composants individuels présentés sur le tableau de bord et les pages de configuration.

Autorisations d'utilisation des fonctionnalités AMS

Pour permettre à vos utilisateurs de lire et de configurer les fonctionnalités d'AMS Accelerate, comme l'accès à la console AMS ou la configuration de sauvegardes, vous devez accorder des autorisations explicites à leurs rôles IAM pour effectuer ces actions. Le AWS CloudFormation modèle suivant contient les politiques requises pour lire et configurer les services associés à AMS

afin que vous puissiez les attribuer à vos rôles IAM. Ils sont conçus pour s'aligner étroitement sur les responsabilités professionnelles courantes dans le secteur informatique, où des autorisations d'administrateur ou de lecture seule sont requises ; toutefois, si vous devez accorder des autorisations différentes aux utilisateurs, vous pouvez modifier la politique pour inclure ou exclure des autorisations spécifiques. Vous pouvez également créer votre propre politique personnalisée.

Le modèle fournit deux politiques. La `AMSAccelerateAdminAccess` politique est destinée à être utilisée pour configurer et faire fonctionner les composants AMS Accelerate. Cette politique est généralement adoptée par un administrateur informatique et accorde des autorisations pour configurer les fonctionnalités AMS telles que les correctifs et les sauvegardes. `AMSAccelerateReadOnly`accorde les autorisations minimales requises pour consulter les ressources liées à AMS Accelerate.

```
AWSTemplateFormatVersion: 2010-09-09
Description: AMSAccelerateCustomerAccessPolicies

Resources:
  AMSAccelerateAdminAccess:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateAdminAccess
      Path: /
      PolicyDocument:
        Fn::Sub:
        - |
          {
            "Version": "2012-10-17",
            "Statement": [
              {
                 "Sid": "AmsSelfServiceReport",
                 "Effect": "Allow",
                 "Action": "amsssrv:*",
                 "Resource": "*"
              },
              {
                "Sid": "AmsBackupPolicy",
                "Effect": "Allow",
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::${AWS::AccountId}:role/ams-backup-iam-role"
              },
              {
                "Sid": "AmsChangeRecordKMSPolicy",
```

```
                "Effect": "Allow",
                "Action": [
                  "kms:Encrypt",
                  "kms:Decrypt",
                  "kms:GenerateDataKey"
                ],
                "Resource": [
                  "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
                ],
                "Condition": {
                  "ForAnyValue:StringLike": {
                    "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
                  }
                }
              },
              {
                "Sid": "AmsChangeRecordAthenaReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "athena:BatchGetNamedQuery",
                  "athena:Get*",
                  "athena:List*",
                  "athena:StartQueryExecution",
                  "athena:UpdateWorkGroup",
                  "glue:GetDatabase*",
                  "glue:GetTable*",
                  "s3:GetAccountPublicAccessBlock",
                  "s3:ListAccessPoints",
                  "s3:ListAllMyBuckets"
                ],
                "Resource": "*"
              },
              {
                "Sid": "AmsChangeRecordS3ReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "s3:Get*",
                  "s3:List*"
                ],
                "Resource": [
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/
*",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
```

```
        "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
      ]
    },
    {
      "Sid": "AmsChangeRecordS3WritePolicy",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectLegalHold",
        "s3:PutObjectRetention"

      ],
      "Resource": [
        "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
      ]
    },
    {
      "Sid": "MaciePolicy",
      "Effect": "Allow",
      "Action": [
        "macie2:GetFindingStatistics"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GuardDutyPolicy",
      "Effect": "Allow",
      "Action": [
        "guardduty:GetFindingsStatistics",
        "guardduty:ListDetectors"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SupportPolicy",
      "Effect": "Allow",
      "Action": "support:*",
      "Resource": "*"
    },
    {
      "Sid": "ConfigPolicy",
      "Effect": "Allow",
      "Action": [
        "config:Get*",
```

```
                "config:Describe*",
                "config:Deliver*",
                "config:List*",
                "config:StartConfigRulesEvaluation"
              ],
              "Resource": "*"
            },
            {
              "Sid": "AppConfigReadPolicy",
              "Effect": "Allow",
              "Action": [
                "appconfig:List*",
                "appconfig:Get*"
              ],
              "Resource": "*"
            },
            {
              "Sid": "AppConfigPolicy",
              "Effect": "Allow",
              "Action": [
                "appconfig:StartDeployment",
                "appconfig:StopDeployment",
                "appconfig:CreateHostedConfigurationVersion",
                "appconfig:ValidateConfiguration"
              ],
              "Resource": [
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/configurationprofile/
${AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID}",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/environment/*",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/configurationprofile/
${AMSResourceTaggerConfigurationCustomerManagedTagsProfileID}",
                "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/environment/*",
                "arn:aws:appconfig:*:${AWS::AccountId}:deploymentstrategy/*"
              ]
            },
            {
```

```
      "Sid": "CloudFormationStacksPolicy",
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EC2Policy",
      "Action": [
        "ec2:DescribeInstances"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "SSMPolicy",
      "Effect": "Allow",
      "Action": [
        "ssm:AddTagsToResource",
        "ssm:CancelCommand",
        "ssm:CancelMaintenanceWindowExecution",
        "ssm:CreateAssociation",
        "ssm:CreateAssociationBatch",
        "ssm:CreateMaintenanceWindow",
        "ssm:CreateOpsItem",
        "ssm:CreatePatchBaseline",
        "ssm:DeleteAssociation",
        "ssm:DeleteMaintenanceWindow",
        "ssm:DeletePatchBaseline",
        "ssm:DeregisterPatchBaselineForPatchGroup",
        "ssm:DeregisterTargetFromMaintenanceWindow",
        "ssm:DeregisterTaskFromMaintenanceWindow",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "ssm:PutConfigurePackageResult",
        "ssm:RegisterDefaultPatchBaseline",
        "ssm:RegisterPatchBaselineForPatchGroup",
        "ssm:RegisterTargetWithMaintenanceWindow",
        "ssm:RegisterTaskWithMaintenanceWindow",
        "ssm:RemoveTagsFromResource",
        "ssm:SendCommand",
        "ssm:StartAssociationsOnce",
```

```
            "ssm:StartAutomationExecution",
            "ssm:StartSession",
            "ssm:StopAutomationExecution",
            "ssm:TerminateSession",
            "ssm:UpdateAssociation",
            "ssm:UpdateAssociationStatus",
            "ssm:UpdateMaintenanceWindow",
            "ssm:UpdateMaintenanceWindowTarget",
            "ssm:UpdateMaintenanceWindowTask",
            "ssm:UpdateOpsItem",
            "ssm:UpdatePatchBaseline"
          ],
          "Resource": "*"
        },
        {
          "Sid": "AmsPatchRestrictAMSResources",
          "Effect": "Deny",
          "Action": [
            "ssm:DeletePatchBaseline",
            "ssm:UpdatePatchBaseline"
          ],
          "Resource": [
            "arn:aws:ssm:${AWS::Region}:${AWS::AccountId}:patchbaseline/*"
          ],
          "Condition": {
            "StringLike": {
              "aws:ResourceTag/ams:resourceOwner": "*"
            }
          }
        },
        {
          "Sid": "AmsPatchRestrictAmsTags",
          "Effect": "Deny",
          "Action": [
            "ssm:AddTagsToResource",
            "ssm:RemoveTagsFromResource"
          ],
          "Resource": "*",
          "Condition": {
            "ForAnyValue:StringLike": {
              "aws:TagKeys": [
                "AMS*",
                "Ams*",
                "ams*"
```

```
            ]
          }
        }
      },
      {
        "Sid": "TagReadPolicy",
        "Effect": "Allow",
        "Action": [
          "tag:GetResources",
          "tag:GetTagKeys"
        ],
        "Resource": "*"
      },
      {
        "Sid": "CloudtrailReadPolicy",
        "Effect": "Allow",
        "Action": [
          "cloudtrail:DescribeTrails",
          "cloudtrail:GetTrailStatus",
          "cloudtrail:LookupEvents"
        ],
        "Resource": "*"
      },
      {
        "Sid": "EventBridgePolicy",
        "Effect": "Allow",
        "Action": [
          "events:Describe*",
          "events:List*",
          "events:TestEventPattern"
        ],
        "Resource": "*"
      },
      {
        "Sid": "IAMReadOnlyPolicy",
        "Action": [
            "iam:ListRoles",
            "iam:GetRole"
        ],
        "Effect": "Allow",
        "Resource": "*"
      },
      {
        "Sid": "AmsResourceSchedulerPassRolePolicy",
```

```
                "Effect": "Allow",
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::${AWS::AccountId}:role/
ams_resource_scheduler_ssm_automation_role",
                "Condition": {
                    "StringEquals": {
                        "iam:PassedToService": "ssm.amazonaws.com"
                    }
                }
              }
            ]
          }
        - AMSAlarmManagerConfigurationApplicationId: !ImportValue "AMS-Alarm-Manager-
Configuration-ApplicationId"
          AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID: !ImportValue
 "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID"
          AMSResourceTaggerConfigurationApplicationId: !ImportValue "AMS-
ResourceTagger-Configuration-ApplicationId"
          AMSResourceTaggerConfigurationCustomerManagedTagsProfileID: !ImportValue
 "AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID"

  AMSAccelerateReadOnly:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateReadOnly
      Path: /
      PolicyDocument: !Sub |
        {
          "Version": "2012-10-17",
          "Statement": [
          {
                 "Sid": "AmsSelfServiceReport",
                 "Effect": "Allow",
                 "Action": "amsssrv:*",
                 "Resource": "*"
              },
            {
               "Sid": "AmsBackupPolicy",
               "Effect": "Allow",
               "Action": [
                 "backup:Describe*",
                 "backup:Get*",
                 "backup:List*"
               ],
```

```
            "Resource": "*"
        },
        {
            "Action": [
                "rds:DescribeDBSnapshots",
                "rds:ListTagsForResource",
                "rds:DescribeDBInstances",
                "rds:describeDBSnapshots",
                "rds:describeDBEngineVersions",
                "rds:describeOptionGroups",
                "rds:describeOrderableDBInstanceOptions",
                "rds:describeDBSubnetGroups",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBClusterParameterGroups",
                "rds:DescribeDBInstanceAutomatedBackups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "dynamodb:ListBackups",
                "dynamodb:ListTables"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "elasticfilesystem:DescribeFilesystems"
            ],
            "Resource": "arn:aws:elasticfilesystem:*:*:file-system/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DescribeVolumes",
                "ec2:describeAvailabilityZones",
                "ec2:DescribeVpcs",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeSecurityGroups",
```

```
                "ec2:DescribeImages",
                "ec2:DescribeSubnets",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:GetResources"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:DescribeCachediSCSIVolumes",
                "storagegateway:DescribeStorediSCSIVolumes"
            ],
            "Resource": "arn:aws:storagegateway:*:*:gateway/*/volume/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Resource": "arn:aws:storagegateway:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:DescribeGatewayInformation",
                "storagegateway:ListVolumes",
                "storagegateway:ListLocalDisks"
            ],
            "Resource": "arn:aws:storagegateway:*:*:gateway/*"
        },
        {
            "Action": [
```

```
                "iam:ListRoles",
                "iam:GetRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "organizations:DescribeOrganization",
            "Resource": "*"
        },
        {
            "Action": "fsx:DescribeBackups",
            "Effect": "Allow",
            "Resource": "arn:aws:fsx:*:*:backup/*"
        },
        {
            "Action": "fsx:DescribeFileSystems",
            "Effect": "Allow",
            "Resource": "arn:aws:fsx:*:*:file-system/*"
        },
        {
            "Action": "ds:DescribeDirectories",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
          "Sid": "AmsChangeRecordKMSPolicy",
          "Effect": "Allow",
          "Action": [
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:GenerateDataKey"
          ],
          "Resource": [
            "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
          ],
          "Condition": {
            "ForAnyValue:StringLike": {
              "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
            }
          }
        },
        {
```

```
      "Sid": "AmsChangeRecordAthenaReadPolicy",
      "Effect": "Allow",
      "Action": [
        "athena:BatchGetNamedQuery",
        "athena:Get*",
        "athena:List*",
        "athena:StartQueryExecution",
        "athena:UpdateWorkGroup",
        "glue:GetDatabase*",
        "glue:GetTable*",
        "s3:GetAccountPublicAccessBlock",
        "s3:ListAccessPoints",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AmsChangeRecordS3ReadPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": [
        "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
        "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*",
        "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
        "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
      ]
    },
    {
      "Sid": "AmsChangeRecordS3WritePolicy",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectLegalHold",
        "s3:PutObjectRetention"
      ],
      "Resource": [
        "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
      ]
    },
    {
      "Sid": "MaciePolicy",
```

```
            "Effect": "Allow",
            "Action": [
              "macie2:GetFindingStatistics"
            ],
            "Resource": "*"
          },
          {
            "Sid": "GuardDutyReadPolicy",
            "Effect": "Allow",
            "Action": [
              "guardduty:GetFindingsStatistics",
              "guardduty:ListDetectors"
            ],
            "Resource": "*"
          },
          {
            "Sid": "SupportReadPolicy",
            "Effect": "Allow",
            "Action": "support:Describe*",
            "Resource": "*"
          },
          {
            "Sid": "ConfigReadPolicy",
            "Effect": "Allow",
            "Action": [
              "config:Get*",
              "config:Describe*",
              "config:List*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "AppConfigReadPolicy",
            "Effect": "Allow",
            "Action": [
              "appconfig:List*",
              "appconfig:Get*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "CloudFormationReadPolicy",
            "Effect": "Allow",
            "Action": [
```

```
            "cloudformation:DescribeStacks"
          ],
          "Resource": "*"
        },
        {
          "Sid": "EC2ReadPolicy",
          "Effect": "Allow",
          "Action": [
            "ec2:DescribeInstances"
          ],
          "Resource": "*"
        },
        {
          "Sid": "SSMReadPolicy",
          "Effect": "Allow",
          "Action": [
            "ssm:Describe*",
            "ssm:Get*",
            "ssm:List*"
          ],
          "Resource": "*"
        },
        {
          "Sid": "TagReadPolicy",
          "Effect": "Allow",
          "Action": [
            "tag:GetResources",
            "tag:GetTagKeys"
          ],
          "Resource": "*"
        },
        {
          "Sid": "CloudtrailReadPolicy",
          "Effect": "Allow",
          "Action": [
            "cloudtrail:DescribeTrails",
            "cloudtrail:GetTrailStatus",
            "cloudtrail:LookupEvents"
          ],
          "Resource": "*"
        },
        {
          "Sid": "EventBridgePolicy",
          "Effect": "Allow",
```

```
            "Action": [
              "events:Describe*",
              "events:List*",
              "events:TestEventPattern"
            ],
            "Resource": "*"
          }
        ]
      }
```

Pourquoi et quand AMS accède à votre compte

Les opérateurs AMS Accelerate (Accelerate) peuvent accéder à la console de votre compte et aux instances, dans certaines circonstances, pour gérer vos ressources. Ces événements d'accès sont documentés dans vos journaux AWS CloudTrail (CloudTrail). Pour plus de détails sur la façon de vérifier l'activité de votre compte par l'équipe AMS Accelerate Operations et sur l'automatisation d'AMS Accelerate, consultezSuivi des modifications apportées à vos comptes AMS Accelerate.

Pourquoi, quand et comment AMS accède à votre compte sont expliqués dans les rubriques suivantes.

Déclencheurs d'accès au compte client AMS

L'activité d'accès au compte client AMS est déterminée par des déclencheurs. Les déclencheurs actuels sont les AWS tickets créés dans notre système de gestion des problèmes en réponse aux alarmes et aux événements d'Amazon CloudWatch (CloudWatch), ainsi que les rapports d'incidents ou les demandes de service que vous soumettez. Plusieurs appels de service et activités au niveau de l'hôte peuvent être effectués pour chaque accès.

La justification de l'accès, les déclencheurs et l'initiateur du déclencheur sont répertoriés dans le tableau suivant.

déclencheurs d'accès

Accès	Initiateur	Déclencheur
Corriger	AMS	Problème lié au correctif
Enquête sur un problème interne	AMS	Problème (problème identifié comme systémique)

Accès	Initiateur	Déclencheur
Enquête sur les alertes et mesures correctives	AMS	Éléments de travail opérationnels (SSM OpsItems) d'AWS Systems Manager
Enquête sur les incidents et résolution des incidents	Vous	Dossier d'assistance entrant (un incident ou une demande de service que vous soumettez)
Traitement des demandes de service entrantes	Vous	

Accès au compte client AMS | Rôles IAM

Les opérateurs AMS ont besoin des rôles suivants pour gérer votre compte.

> **Note**
>
> Les rôles d'accès AMS permettent aux opérateurs AMS d'accéder à vos ressources pour fournir des fonctionnalités AMS (voirService description (Description du service)). La modification de ces rôles peut entraver notre capacité à fournir ces capacités. Si vous devez modifier les rôles d'accès AMS, consultez votre architecte cloud.

Rôles IAM pour l'accès AMS aux comptes clients

Nom du rôle	Description
ams-access-admin	Ce rôle dispose d'un accès administratif complet à votre compte sans restrictions. Les services AMS utilisent ce rôle avec des politiques de session restrictives qui limitent l'accès au déploiement de l'infrastructure AMS et à l'exploitation de votre compte.
ams-access-admin-operations	Ce rôle accorde aux opérateurs AMS des autorisations administratives pour gérer votre compte. Ce rôle n'accorde pas d'autorisation de lecture, d'écriture ou de suppression du contenu client dans les AWS

Nom du rôle	Description
	services couramment utilisés comme magasins de données, tels qu'Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift et Amazon. ElastiCache Seuls les opérateurs AMS qualifiés ayant une solide connaissance et une solide expérience de la gestion des accès peuvent assumer ce rôle. Ces opérateur s servent de point d'escalade pour les problèmes de gestion des accès et accèdent à vos comptes pour résoudre les problèmes d'accès des opérateurs AMS.
ams-access-management	Déployé manuellement lors de l'intégration. Le système AMS Access nécessite ce rôle pour la gestion `ams-access-roles` et le `ams-access-managed-policies` cumul.
ams-access-operations	Ce rôle est autorisé à effectuer des tâches administr atives dans vos comptes. Ce rôle ne dispose pas d'autorisations de lecture, d'écriture ou de suppression du contenu client dans les AWS services couramment utilisés comme magasins de données, tels qu'Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift et Amazon. ElastiCache Les autorisations permettant d'effectuer des opérations d' AWS Identity and Access Management écriture sont également exclues de ce rôle. Le personnel des opérations d'AMS Accelerate et les architectes du cloud (CAs) peuvent assumer ce rôle.

Nom du rôle	Description
ams-access-read-only	Ce rôle dispose d'un accès en lecture seule à votre compte. Le personnel des opérations d'AMS Accelerat e et les architectes du cloud (CAs) peuvent assumer ce rôle. Les autorisations de lecture du contenu client dans les AWS services couramment utilisés comme magasins de données, tels qu'Amazon S3, Amazon RDS, DynamoDB, Amazon Redshift, etc. ne se voient pas attribuer ElastiCache ce rôle.
ams-access-security-analyst	Ce rôle de sécurité AMS est autorisé dans votre compte AMS à effectuer une surveillance dédiée des alertes de sécurité et à la gestion des incidents de sécurité. Seules quelques personnes sélectionnées d'AMS Security peuvent assumer ce rôle.
ams-access-security-analyst-lecture seule	Ce rôle de sécurité AMS est limité aux autorisations en lecture seule de votre compte AMS pour effectuer une surveillance dédiée des alertes de sécurité et une gestion des incidents de sécurité.

> **Note**
>
> Il s'agit du modèle du ams-access-management rôle. Il s'agit de la pile que les architectes du cloud (CAs) déploient manuellement dans votre compte au moment de l'intégration : management-role.yaml.
> Il s'agit du modèle pour les différents rôles d'accès pour les différents niveaux d'accès : ams-access-read-only,, ams-access-operations ams-access-admin-operations, ams-access-admin : accelerate-roles.yaml.

Comment AMS accède à votre compte

Les opérateurs AMS Accelerate peuvent accéder à la console et aux instances de votre compte, dans certaines circonstances.

Les opérateurs AMS utilisent le service d'accès interne AMS Accelerate pour accéder à vos comptes de manière sécurisée et auditée. Pour accéder à vos instances, les opérateurs AMS utilisent le même service d'accès AMS interne que le courtier et, une fois l'accès accordé, les opérateurs AMS Accelerate utilisent le gestionnaire de sessions SSM pour accéder à l'aide des informations d'identification de session. L'accès RDP pour les instances Windows est fourni en établissant une redirection de port vers l'instance et en créant un utilisateur local à l'aide de SSM. Les informations d'identification de l'utilisateur local sont utilisées pour l'accès RDP et sont supprimées à la fin de la session.

Comment et quand utiliser le compte utilisateur root dans AMS

L'utilisateur root est le superutilisateur de votre AWS compte. AMS surveille l'utilisation du root. Nous vous recommandons d'utiliser root uniquement pour les quelques tâches qui le nécessitent, par exemple : modifier les paramètres de votre compte, activer l'accès AWS Identity and Access Management (IAM) à la facturation et à la gestion des coûts, modifier votre mot de passe root et activer l'authentification multifactorielle (MFA). Consultez la section Tâches nécessitant des informations d'identification de l'utilisateur root dans le guide de AWS Identity and Access Management l'utilisateur.

Rootez avec AMS Accelerate :

AMS ne vous interdit pas d'utiliser votre compte utilisateur root. Cependant, AMS Operations and Security considère son utilisation comme un problème à étudier et nous contacterons votre équipe de sécurité à chaque utilisation.

Nous vous recommandons de contacter votre CSDM et votre CA vingt-quatre heures à l'avance pour les informer du travail d'accès root que vous avez l'intention d'effectuer.

Opérations AMS et réponse de sécurité à l'utilisation par le root :

AMS reçoit une alarme lorsque le compte utilisateur root est utilisé. Si l'utilisation des informations d'identification root n'est pas planifiée, ils contactent l'équipe de sécurité AMS et l'équipe chargée de votre compte pour vérifier s'il s'agit d'une activité attendue. Si aucune activité n'est prévue, AMS travaille avec votre équipe de sécurité pour étudier le problème.

Gestion de la sécurité dans AMS Accelerate

AWS Managed Services utilise de multiples contrôles pour protéger vos actifs informationnels et vous aider à garantir la sécurité de votre AWS infrastructure. AMS Accelerate gère une bibliothèque AWS Config Rules de mesures correctives pour garantir que tous vos comptes sont conformes aux normes du secteur en matière de sécurité et d'intégrité opérationnelle. AWS Config Rules suit en permanence le changement de configuration parmi vos ressources enregistrées. Si une modification enfreint l'une des conditions des règles, AMS communique ses conclusions et vous permet de remédier aux violations automatiquement ou sur demande, en fonction de la gravité de la violation. AWS Config Rules faciliter le respect des normes établies par : le Center for Internet Security (CIS), le cadre de sécurité cloud (CSF) du National Institute of Standards and Technology (NIST), le Health Insurance Portability and Accountability Act (HIPAA) et le standard de sécurité des données (DSS) du secteur des cartes de paiement (PCI).

En outre, AMS utilise Amazon GuardDuty pour identifier les activités potentiellement non autorisées ou malveillantes dans votre AWS environnement. AMS surveille les GuardDuty résultats 24 heures sur 24, 7 jours sur 7. AMS collabore avec vous pour comprendre l'impact des résultats et identifier les mesures correctives en fonction des recommandations des meilleures pratiques. AMS utilise également Amazon Macie pour protéger vos données sensibles telles que les informations médicales personnelles (PHI), les informations personnelles identifiables (PII) et les données financières.

> **Note**
>
> Amazon Macie est un service optionnel qui n'est pas activé par défaut.

AMS Accelerate fournit une gamme de services opérationnels pour vous aider à atteindre l'excellence opérationnelle sur AWS. Pour en savoir plus sur la façon dont AMS aide vos équipes à atteindre l'excellence opérationnelle globale AWS Cloud grâce à ses fonctionnalités opérationnelles clés, notamment le service d'assistance 24 heures sur 24, 7 jours sur 7, la surveillance proactive, la sécurité, l'application de correctifs, la journalisation et la sauvegarde, consultez les diagrammes d'architecture de référence AMS.

Rubriques

- Utilisez le document Log4j SSM pour découvrir les occurrences dans Accelerate
- Surveillance de la sécurité de l'infrastructure dans AMS

- Protection des données dans Accelerate
- AWS Identity and Access Management dans AMS Accelerate
- Réponse aux incidents de sécurité dans AMS
- Enregistrement et surveillance des événements de sécurité dans Accelerate
- Conformité des configurations dans Accelerate
- Réponse aux incidents dans Accelerate
- Résilience dans Accelerate
- Contrôle de sécurité pour les systèmes end-of-support d'exploitation
- Bonnes pratiques en matière de sécurité dans Accelerate
- Examens de sécurité des demandes de modification
- FAQ sur la sécurité

Utilisez le document Log4j SSM pour découvrir les occurrences dans Accelerate

Le document Log4j (AWS Systems Manager document SSM) vous aide à rechercher la bibliothèque Apache Log4j2 dans les charges de travail ingérées. Le document d'automatisation fournit un rapport sur l'ID de processus des applications Java dans lesquelles la bibliothèque Log4j2 est active.

Le rapport inclut des informations sur les archives Java (fichiers JAR), trouvées dans l'environnement spécifié qui contient la JndiLookup classe. Il est recommandé de mettre à niveau les bibliothèques découvertes vers la dernière version disponible. Cette mise à niveau atténue l'exécution de code à distance (RCE) identifiée par le biais du CVE-2021-44228. Téléchargez la dernière version de la bibliothèque Log4j depuis Apache. Pour plus d'informations, voir Télécharger Apache Log4j 2.

Le document est partagé avec toutes les régions intégrées à Accelerate,. Pour accéder au document, procédez comme suit :

1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Dans le panneau de navigation, cliquez sur Documents.
3. Choisissez Partagé avec moi.
4. Dans le champ de recherche, saisissez AWSManagedServices-GatherLog4JInformation.
5. Utilisez le contrôle du débit pour exécuter le document à grande échelle.

Le document AWSManagedServices-GatherLog 4JInformation rassemble les paramètres suivants :

- InstanceId: (Obligatoire) ID de votre EC2 instance.
- S3Bucket : (Facultatif) URL pré-signée S3 ou URI S3 (s3://BUCKET_NAME) vers laquelle télécharger les résultats.
- AutomationAssumeRole: (Obligatoire) L'ARN du rôle qui permet à l'automatisation d'effectuer des actions en votre nom.

Il est recommandé d'exécuter ce document à l'aide du contrôle du débit. Vous pouvez définir le paramètre de contrôle du débit comme étant le InstanceIdet lui attribuer soit une liste d'instances, soit appliquer une combinaison balise-touche pour cibler toutes les EC2 instances dotées d'une certaine balise. AWS Managed Services vous recommande également de fournir un bucket Amazon Simple Storage Service (Amazon S3) dans lequel télécharger les résultats, afin de pouvoir créer un rapport à partir des données stockées dans S3. Pour un exemple de la façon d'agréger les résultats dans S3, voir EC2 Instance Stack | Gather Log4j Information.

Si vous ne parvenez pas à mettre à jour le package, suivez les instructions décrites dans la section AWS Sécurité de l'article Utilisation des services de AWS sécurité pour vous protéger contre la vulnérabilité Log4j, la détecter et y répondre. Pour atténuer les vulnérabilités en supprimant la fonctionnalité de JndiLookup classe, exécutez le hot patch Log4j en ligne avec vos applications Java. Pour plus d'informations sur le hot patch, consultez Hotpatch pour Apache Log4j.

Pour toute question concernant le résultat de l'automatisation ou la manière de procéder à des mesures d'atténuation supplémentaires, soumettez une demande de service.

Surveillance de la sécurité de l'infrastructure dans AMS

Lorsque vous intégrez AMS Accelerate et que vous AWS déployez l'infrastructure AWS Config de base et l'ensemble de règles suivants, AMS Accelerate utilise ces règles pour surveiller vos comptes.

- AWS Config rôle lié au service : AMS Accelerate déploie le rôle lié au service nommé AWSServiceRoleForConfig, qui est utilisé pour demander l'état AWS Config d'autres services. AWS Le rôle AWSServiceRoleForConfiglié au service fait confiance au AWS Config service pour assumer le rôle. La politique d'autorisations pour le AWSServiceRoleForConfigrôle contient des autorisations en lecture seule et en écriture seule sur les ressources et des autorisations en lecture seule pour les AWS Config ressources des autres services pris en charge. AWS Config Si vous avez déjà configuré un rôle avec AWS Config Recorder, AMS Accelerate vérifie que le rôle

existant est associé à une politique de gestion AWS Config. Dans le cas contraire, AMS Accelerate remplace le rôle par le rôle lié au service. AWSServiceRoleForConfig

- AWS Config enregistreur et canal de diffusion : AWS Config utilise l'enregistreur de configuration pour détecter les modifications apportées à la configuration de vos ressources et capturer ces modifications sous forme d'éléments de configuration. AMS Accelerate déploie l'enregistreur de configuration dans tous les services Régions AWS, avec un enregistrement continu de toutes les ressources. AMS Accelerate crée également le canal de distribution de configuration, un compartiment Amazon S3, qui est utilisé pour enregistrer les modifications apportées à vos AWS ressources. L'enregistreur de configuration met à jour les états de configuration via le canal de distribution. L'enregistreur de configuration et le canal de diffusion sont nécessaires AWS Config pour fonctionner. AMS Accelerate crée l'enregistreur Régions AWS en tout et un canal de diffusion en un seul Région AWS. Si vous avez déjà un enregistreur et un canal de diffusion dans un Région AWS, AMS Accelerate ne supprime pas les AWS Config ressources existantes. AMS Accelerate utilise plutôt votre enregistreur et votre canal de diffusion existants après avoir vérifié qu'ils sont correctement configurés. Pour plus d'informations sur la manière de réduire AWS Config les coûts, consultezRéduisez AWS Config les coûts dans Accelerate.
- AWS Config règles : AMS Accelerate gère une bibliothèque de mesures correctives AWS Config Rules et de mesures correctives pour vous aider à vous conformer aux normes du secteur en matière de sécurité et d'intégrité opérationnelle. AWS Config Rules suit en permanence les modifications de configuration parmi vos ressources enregistrées. Si une modification enfreint l'une des conditions des règles, AMS communique ses conclusions et vous permet de remédier aux violations automatiquement ou sur demande, en fonction de la gravité de la violation. AWS Config Rules faciliter le respect des normes établies par : le Center for Internet Security (CIS), le cadre de sécurité cloud (CSF) du National Institute of Standards and Technology (NIST), le Health Insurance Portability and Accountability Act (HIPAA) et le standard de sécurité des données (DSS) du secteur des cartes de paiement (PCI).
- AWS Config autorisation d'agrégateur : un agrégateur est un type de AWS Config ressource qui collecte des données de AWS Config configuration et de conformité à partir de plusieurs comptes et de plusieurs régions. AMS Accelerate intègre votre compte à un agrégateur de configuration à partir duquel AMS Accelerate agrège les informations de configuration des ressources de votre compte et les données de conformité des configurations et génère le rapport de conformité. Si des agrégateurs existants sont configurés dans le compte appartenant à AMS, AMS Accelerate déploie un agrégateur supplémentaire et l'agrégateur existant n'est pas modifié.

> **Note**
>
> L'agrégateur Config n'est pas configuré dans vos comptes ; il est plutôt configuré dans les comptes appartenant à AMS et vos comptes y sont intégrés.

Pour en savoir plus AWS Config, consultez :

- AWS Config: Qu'est-ce que Config ?
- AWS Config Rules: Évaluation des ressources à l'aide de règles
- AWS Config Rules: Vérification dynamique de la conformité : AWS Config Rules — Vérification dynamique de la conformité pour les ressources du cloud
- AWS Config Agrégateur : agrégation de données multicomptes et multirégions

Pour plus d'informations sur les rapports, voirAWS Config Rapport de conformité des contrôles.

Utilisation de rôles liés à un service pour AMS Accelerate

AMS Accelerate utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service (SLR) est un type unique de rôle IAM directement lié à AMS Accelerate. Les rôles liés à un service sont prédéfinis par AMS Accelerate 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 d'AMS Accelerate, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AMS Accelerate définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AMS Accelerate peut assumer 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 la section AWS Services qui fonctionnent avec IAM et recherchez les services dont la valeur est Oui dans la colonne Rôles liés à un service. Choisissez un Oui ayant un lien permettant de consulter les détails du rôle pour ce service.

Rôle lié au service du kit de déploiement pour AMS Accelerate

AMS Accelerate utilise le rôle lié au service (SLR) nommé AWSServiceRoleForAWSManagedServicesDeploymentToolkit: ce rôle déploie l'infrastructure AMS Accelerate dans les comptes clients.

> **Note**
>
> Cette politique a récemment été mise à jour ; pour plus de détails, voirAccélérez les mises à jour des rôles liés aux services.

Boîte à outils de déploiement AMS Accelerate SLR

Le rôle AWSService RoleFor AWSManaged ServicesDeploymentToolkit lié à un service fait confiance aux services suivants pour assumer le rôle :

- `deploymenttoolkit.managedservices.amazonaws.com`

La politique nommée AWSManagedServicesDeploymentToolkitPolicypermet à AMS Accelerate d'effectuer des actions sur les ressources suivantes :

- `arn:aws*:s3:::ams-cdktoolkit*`
- `arn:aws*:cloudformation:*:*:stack/ams-cdk-toolkit*`
- `arn:aws:ecr:*:*:repository/ams-cdktoolkit*`

Ce SLR accorde à Amazon S3 l'autorisation de créer et de gérer le compartiment de déploiement utilisé par AMS pour télécharger des ressources, telles que des CloudFormation modèles ou des ensembles d'actifs Lambda, dans le compte pour les déploiements de composants. Ce SLR accorde des CloudFormation autorisations pour déployer la CloudFormation pile qui définit les compartiments de déploiement. Pour plus de détails ou pour télécharger la politique, consultez AWSManagedServices_DeploymentToolkitPolicy.

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 la section Autorisations relatives aux rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'une boîte à outils de déploiement SLR pour AMS Accelerate

Vous n’avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous intégrez AMS dans le AWS Management Console, le ou l' AWS API AWS CLI, AMS Accelerate crée le rôle lié au service pour vous.

> ⚠ Important
>
> Ce rôle lié à un service peut apparaître sur votre compte si vous utilisiez le service AMS Accelerate avant le 9 juin 2022, date à laquelle il a commencé à prendre en charge les rôles liés au service, puis AMS Accelerate a créé le AWSService RoleFor AWSManaged ServicesDeploymentToolkit rôle dans votre compte. Pour en savoir plus, consultez Un nouveau rôle est apparu dans mon compte IAM.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous vous inscrivez à AMS, AMS Accelerate crée à nouveau le rôle lié au service pour vous.

Modification d'un kit de déploiement SLR pour AMS Accelerate

AMS Accelerate ne vous permet pas de modifier le rôle AWSService RoleFor AWSManaged ServicesDeploymentToolkit lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l’aide d’IAM. Pour plus d’informations, consultez Modification d’un rôle lié à un service dans le IAM Guide de l’utilisateur.

Suppression d'un kit de déploiement SLR pour AMS Accelerate

Il n'est pas nécessaire de supprimer le AWSService RoleFor AWSManaged ServicesDeploymentToolkit rôle manuellement. Lorsque vous quittez AMS dans le AWS Management Console, le ou l' AWS API AWS CLI, AMS Accelerate nettoie les ressources et supprime le rôle lié au service pour vous.

Vous pouvez également utiliser la console IAM AWS CLI ou l' AWS API pour supprimer manuellement le rôle lié à un service. Pour cela, vous devez commencer par nettoyer les ressources de votre rôle lié à un service. Vous pouvez ensuite supprimer ce rôle manuellement.

> **Note**
>
> Si le service AMS Accelerate utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources AMS Accelerate utilisées par le rôle lié à AWSService RoleFor AWSManaged ServicesDeploymentToolkit un service

Supprimez la `ams-cdk-toolkit` pile de toutes les régions dans lesquelles votre compte a été intégré dans AMS (vous devrez peut-être d'abord vider manuellement les compartiments S3).

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSService RoleFor AWSManaged ServicesDeploymentToolkit service. Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Detective contrôle le rôle lié au service pour AMS Accelerate

AMS Accelerate utilise le rôle lié au service (SLR) nommé AWSServiceRoleForManagedServices_DetectiveControlsConfig— AWS Managed Services utilise ce rôle lié au service pour déployer l'enregistreur de configuration, les règles de configuration et les contrôles de détection des compartiments S3.

La politique gérée suivante est attachée AWSServiceRoleForManagedServices_DetectiveControlsConfigau rôle lié au service : AWSManagedServices_DetectiveControlsConfig _. ServiceRolePolicy Pour connaître les mises à jour de cette politique, consultez Accélérez les mises à jour des politiques AWS gérées.

Autorisations pour les contrôles de détection SLR pour AMS Accelerate

Le rôle AWSServiceRoleForManagedServices_DetectiveControlsConfig lié à un service fait confiance aux services suivants pour assumer le rôle :

- `detectivecontrols.managedservices.amazonaws.com`

La politique `AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` AWS gérée est associée à ce rôle (voir Le service utilise AWS politique gérée :

AWSManagedServices_DetectiveControlsConfig _ ServiceRolePolicy le rôle pour créer et configurer AMS Detective Controls dans votre compte), ce qui nécessite le déploiement de ressources telles que des compartiments s3, des règles de configuration et un agrégateur. Vous devez configurer les autorisations pour autoriser une entité IAM (telle qu'un utilisateur, un groupe ou un rôle) à créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez la section Autorisations relatives aux rôles liés au service dans le guide de l'utilisateur AWS d'Identity and Access Management.

Création d'un reflex de contrôle de détective pour AMS Accelerate

Vous n’avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous intégrez AMS dans le AWS Management Console, le ou l' AWS API AWS CLI, AMS Accelerate crée le rôle lié au service pour vous.

> **Important**
>
> Ce rôle lié à un service peut apparaître sur votre compte si vous utilisiez le service AMS Accelerate avant le 9 juin 2022, date à laquelle il a commencé à prendre en charge les rôles liés au service, puis AMS Accelerate a créé le AWSServiceRoleForManagedServices_DetectiveControlsConfig rôle dans votre compte. Pour en savoir plus, consultez Un nouveau rôle est apparu dans mon compte IAM.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous vous inscrivez à AMS, AMS Accelerate crée à nouveau le rôle lié au service pour vous.

Modifier un détective contrôle un reflex pour AMS Accelerate

AMS Accelerate ne vous permet pas de modifier le rôle AWSServiceRoleForManagedServices_DetectiveControlsConfig lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l’aide d’IAM. Pour plus d'informations, consultez la section Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer un détective contrôle SLR pour AMS Accelerate

Il n'est pas nécessaire de supprimer le AWSServiceRoleForManagedServices_DetectiveControlsConfig rôle manuellement. Lorsque vous

quittez AMS dans le AWS Management Console, le ou l' AWS API AWS CLI, AMS Accelerate nettoie les ressources et supprime le rôle lié au service pour vous.

Vous pouvez également utiliser la console IAM AWS CLI ou l' AWS API pour supprimer manuellement le rôle lié à un service. Pour cela, vous devez commencer par nettoyer les ressources de votre rôle lié à un service. Vous pouvez ensuite supprimer ce rôle manuellement.

> **Note**
>
> Si le service AMS Accelerate utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources AMS Accelerate utilisées par le rôle lié à AWSServiceRoleForManagedServices_DetectiveControlsConfig un service

Supprimez `ams-detective-controls-config-recorder` `ams-detective-controls-config-rules-cdk` et `ams-detective-controls-infrastructure-cdk` empilez toutes les régions dans lesquelles votre compte a été intégré dans AMS (vous devrez peut-être d'abord vider manuellement les compartiments S3).

Pour supprimer manuellement le rôle lié à un service à l’aide d’IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForManagedServices_DetectiveControlsConfig service. Pour plus d’informations, consultez Suppression d’un rôle lié à un service dans le Guide de l’utilisateur IAM.

Rôle lié au service Amazon EventBridge Rule pour AMS Accelerate

AMS Accelerate utilise le rôle lié au service (SLR) nommé. AWSServiceRoleForManagedServices_Events Ce rôle fait confiance à l'un des responsables du service AWS Managed Services (events.managedservices.amazonaws.com) pour assumer le rôle à votre place. Le service utilise le rôle pour créer une règle EventBridge gérée par Amazon. Cette règle est l'infrastructure requise dans votre compte AWS pour transmettre les informations de changement d'état d'alarme de votre compte à AWS Managed Services.

Autorisations pour EventBridge SLR pour AMS Accelerate

Le rôle AWSServiceRoleForManagedServices_Events lié à un service fait confiance aux services suivants pour assumer le rôle :

- `events.managedservices.amazonaws.com`

La politique `AWSManagedServices_EventsServiceRolePolicy` AWS gérée est associée à ce rôle (voirAWS politique gérée : AWSManagedServices_EventsServiceRolePolicy). Le service utilise ce rôle pour transmettre à AMS les informations de modification de l'état de l'alarme depuis votre compte. 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 AWS Identity and Access Management

Vous pouvez télécharger le JSON AWSManagedServices_EventsServiceRolePolicy dans ce fichier ZIP : EventsServiceRolePolicy.zip.

Création d'un EventBridge reflex pour AMS Accelerate

Vous n’avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous intégrez AMS dans le AWS Management Console, le ou l' AWS API AWS CLI, AMS Accelerate crée le rôle lié au service pour vous.

> **Important**
>
> Ce rôle lié au service peut apparaître sur votre compte si vous utilisiez le service AMS Accelerate avant le 7 février 2023, date à laquelle il a commencé à prendre en charge les rôles liés au service, puis AMS Accelerate a créé le AWSServiceRoleForManagedServices_Events rôle dans votre compte. Pour en savoir plus, consultez Un nouveau rôle est apparu dans mon compte IAM.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous vous inscrivez à AMS, AMS Accelerate crée à nouveau le rôle lié au service pour vous.

Modification d'un EventBridge reflex pour AMS Accelerate

AMS Accelerate ne vous permet pas de modifier le rôle AWSServiceRoleForManagedServices_Events lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l’aide d’IAM. Pour plus d’informations, consultez Modification d’un rôle lié à un service dans le IAM Guide de l’utilisateur.

Supprimer un appareil photo EventBridge reflex pour AMS Accelerate

Il n'est pas nécessaire de supprimer le AWSServiceRoleForManagedServices_Events rôle manuellement. Lorsque vous quittez AMS dans le AWS Management Console, le ou l' AWS API AWS CLI, AMS Accelerate nettoie les ressources et supprime le rôle lié au service pour vous.

Vous pouvez également utiliser la console IAM AWS CLI ou l' AWS API pour supprimer manuellement le rôle lié à un service. Pour cela, vous devez commencer par nettoyer les ressources de votre rôle lié à un service. Vous pouvez ensuite supprimer ce rôle manuellement.

> **Note**
>
> Si le service AMS Accelerate utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources AMS Accelerate utilisées par le rôle lié à AWSServiceRoleForManagedServices_Events un service

Pour supprimer manuellement le rôle lié à un service à l’aide d’IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForManagedServices_Events service. Pour plus d’informations, consultez Suppression d’un rôle lié à un service dans le Guide de l’utilisateur IAM.

Rôle lié au service des contacts pour AMS Accelerate

AMS Accelerate utilise le rôle lié au service (SLR) nommé AWSServiceRoleForManagedServices_Contacts— Ce rôle facilite les notifications automatiques en cas d'incident en permettant au service de lire les balises existantes de la ressource affectée et de récupérer l'e-mail configuré du point de contact approprié.

Il s'agit du seul service qui utilise ce rôle lié au service.

La politique gérée suivante est attachée AWSServiceRoleForManagedServices_Contactsau rôle lié au service :. AWSManagedServices_ContactsServiceRolePolicy Pour connaître les mises à jour de cette politique, consultez Accélérez les mises à jour des politiques AWS gérées.

Autorisations pour les contacts SLR pour AMS Accelerate

Le rôle AWSServiceRoleForManagedServices_Contacts lié à un service fait confiance aux services suivants pour assumer le rôle :

- `contacts-service.managedservices.amazonaws.com`

La politique gérée par `AWSManagedServices_ContactsServiceRolePolicy` AWS est associée à ce rôle (voirAWS politique gérée : AWSManagedServices_ContactsServiceRolePolicy). Le service utilise ce rôle pour lire les balises de n'importe quelle AWS ressource et trouver l'e-mail contenu dans le tag, du point de contact approprié en cas d'incident. Ce rôle facilite les notifications automatisées en cas d'incident en permettant à AMS de lire cette balise sur une ressource affectée et de récupérer l'e-mail. Pour plus d'informations, consultez la section Autorisations relatives aux rôles liés au service dans le guide de l'utilisateur AWS d'Identity and Access Management.

> **Important**
>
> Ne stockez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans des balises. AMS utilise des balises pour vous fournir des services d'administration. Les balises ne sont pas destinées à être utilisées pour des données privées ou sensibles.

La politique d'autorisations de rôle nommée AWSManagedServices_ContactsServiceRolePolicy permet à AMS Accelerate d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : autorise le service Contacts à lire les balises spécifiquement configurées pour contenir l'e-mail permettant à AMS d'envoyer des notifications d'incident sur n'importe quelle ressource AWS.

Vous pouvez télécharger le JSON AWSManagedServices_ContactsServiceRolePolicy dans ce fichier ZIP : ContactsServicePolicy.zip.

Création d'un reflex à contacts pour AMS Accelerate

Vous n’avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous intégrez AMS dans le AWS Management Console, le ou l' AWS API AWS CLI, AMS Accelerate crée le rôle lié au service pour vous.

> **Important**
>
> Ce rôle lié au service peut apparaître sur votre compte si vous utilisiez le service AMS Accelerate avant le 16 février 2023, date à laquelle il a commencé à prendre en charge les rôles liés au service, puis AMS Accelerate a créé le AWSServiceRoleForManagedServices_Contacts rôle dans votre compte. Pour en savoir plus, consultez Un nouveau rôle est apparu dans mon compte IAM.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous vous inscrivez à AMS, AMS Accelerate crée à nouveau le rôle lié au service pour vous.

Modification d'un reflex à contacts pour AMS Accelerate

AMS Accelerate ne vous permet pas de modifier le rôle AWSServiceRoleForManagedServices_Contacts lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le IAM Guide de l'utilisateur.

Supprimer un reflex Contacts pour AMS Accelerate

Il n'est pas nécessaire de supprimer le AWSServiceRoleForManagedServices_Contacts rôle manuellement. Lorsque vous quittez AMS dans le AWS Management Console, le ou l' AWS API AWS CLI, AMS Accelerate nettoie les ressources et supprime le rôle lié au service pour vous.

Vous pouvez également utiliser la console IAM AWS CLI ou l' AWS API pour supprimer manuellement le rôle lié à un service. Pour cela, vous devez commencer par nettoyer les ressources de votre rôle lié à un service. Vous pouvez ensuite supprimer ce rôle manuellement.

> **Note**
>
> Si le service AMS Accelerate utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources AMS Accelerate utilisées par le rôle lié à AWSServiceRoleForManagedServices_Contacts un service

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForManagedServices_Contacts service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés au service AMS Accelerate

AMS Accelerate prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Régions et points de terminaison AWS.

Accélérez les mises à jour des rôles liés aux services

Consultez les détails des mises à jour apportées aux rôles liés au service Accelerate 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 Historique du document pour le guide de l'utilisateur d'AMS Accelerate page Accelerate.

Modification	Description	Date

Politique mise à jour — Boîte à outils de déploiement	• Ces nouvelles autorisations ont été ajoutées pour la ressource `arn:aws:ecr:*:*:repository/ams-cdktoolkit*` :
	`ecr:BatchGetRepositoryScanningConfiguration`
	`ecr:PutImageScanningConfiguration`
		4 avril 2024

Politique mise à jour — Boîte à outils de déploiement	• Ces nouvelles autorisations ont été ajoutées pour la ressource `arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*` :
	`cloudformation:DeleteChangeSet`
	`cloudformation:DescribeStackEvents`
	`cloudformation:GetTemplate`
	`cloudformation:TagResource`
	`cloudformation:UntagResource`
		9 mai 2023

Modification	Description	Date

	• Ces nouvelles autorisations ont été ajoutées pour la ressource `arn:aws:ecr:*:*:repository/ams-cdktoolkit*` :
	
	`ecr:CreateRepository`
	`ecr:DeleteLifecyclePolicy`
	`ecr:DeleteRepository`
	`ecr:DeleteRepositoryPolicy`
	`ecr:DescribeRepositories`
	`ecr:GetLifecyclePolicy`
	`ecr:ListTagsForResource`
	`ecr:PutImageTagMutability`
	`ecr:PutLifecyclePolicy`
	`ecr:SetRepositoryPolicy`
	`ecr:TagResource`
	`ecr:UntagResource`
	
	• En outre, certaines actions existantes comportant un caractère générique ont été réduites à des actions individuelles :
	
	`- s3:DeleteObject*`
	`+ s3:DeleteObject`
	`+ s3:DeleteObjectTagging`
	`+ s3:DeleteObjectVersion`
	`+ s3:DeleteObjectVersionTagging`
	
	`- s3:GetObject*`
	`+ s3:GetObject`
	`+ s3:GetObjectAcl`
	`+ s3:GetObjectAttributes`
	`+ s3:GetObjectLegalHold`
	`+ s3:GetObjectRetention`
	`+ s3:GetObjectTagging`
	`+ s3:GetObjectVersion`
	`+ s3:GetObjectVersionAcl`
	`+ s3:GetObjectVersionAttributes`
	`+ s3:GetObjectVersionForReplication`
	`+ s3:GetObjectVersionTagging`
	`+ s3:GetObjectVersionTorrent`	

Modification	Description	Date

	<pre>- cloudformation:UpdateTermination*
	+ cloudformation:UpdateTerminationProtection</pre>	

Politique mise à jour — Detective Controls	• Les CloudFormation actions ont été précisées après confirmation auprès de l'équipe chargée de la sécurité et de l'accès. • Les actions Lambda ont été supprimées de la politique car elles n'ont aucun impact sur l'embarquement onboarding/off	10 avril 2023
Politique mise à jour — Detective Controls	Mise à jour de la politique et ajout de la politique de limites des autorisations.	21 mars 2023
Nouveau rôle lié à un service — Contacts SLR	Accelerate a ajouté un nouveau rôle lié au service Contacts. Ce rôle facilite les notifications automatisées en cas d'incident en permettant au service de lire les balises existantes de la ressource affectée et de récupérer l'e-mail configuré du point de contact approprié.	16 février 2023
Nouveau rôle lié au service — EventBridge	Accelerate a ajouté un nouveau rôle lié à un service pour une règle Amazon EventBridge . Ce rôle fait confiance à l'un des responsables du service AWS Managed Services (events.managedservices.amazonaws.com) pour assumer le rôle à votre place. Le service utilise le rôle pour créer une règle EventBridge gérée par Amazon. Cette règle est l'infrastructure requise dans votre compte AWS pour transmettre les informations de changement d'état d'alarme de votre compte à AWS Managed Services.	7 février 2023

Modification	Description	Date
Rôle lié au service mis à jour : boîte à outils de déploiement	Accélérez les mises à jour AWSService RoleFor AWSManaged ServicesDeploymentToolkit avec les nouvelles autorisations S3. Ces nouvelles autorisations ont été ajoutées : `"s3:GetLifecycleConfiguration", "s3:GetBucketLogging", "s3:ListBucket", "s3:GetBucketVersioning", "s3:PutLifecycleConfiguration", "s3:GetBucketLocation", "s3:GetObject*"`	30 janvier 2023
Accélérez le suivi initial des modifications	Accelerate a commencé à suivre les modifications apportées à ses rôles liés aux services.	30 novembre 2022
Nouveau rôle lié au service — Detective Controls	Accelerate a ajouté un nouveau rôle lié au service pour déployer les contrôles Accelerate Detective. AWS Managed Services utilise ce rôle lié au service pour déployer l'enregistreur de configuration, les règles de configuration et les contrôles de détection des compartim ents S3.	13 octobre 2022
Nouveau rôle lié au service : boîte à outils de déploiement	Accelerate a ajouté un nouveau rôle lié au service pour déployer l'infrastructure Accelerate. ce rôle déploie l'infrastructure AMS Accelerate dans les comptes clients.	9 juin 2022

AWS politiques gérées pour AMS Accelerate

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 Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Pour un tableau des modifications, voirAccélérez les mises à jour des politiques AWS gérées.

AWS politique gérée : AWSManagedServices_AlarmManagerPermissionsBoundary

AWS Managed Services (AMS) utilise la politique `AWSManagedServices_AlarmManagerPermissionsBoundary` AWS gérée.
Cette politique AWS gérée est utilisée dans le AWSManagedServices_AlarmManager
_ ServiceRolePolicy pour restreindre les autorisations des rôles IAM créés par.
AWSServiceRoleForManagedServices_AlarmManager

Cette politique accorde aux rôles IAM créés dans le cadre deComment fonctionne Alarm Manager, les autorisations nécessaires pour effectuer des opérations telles que l'évaluation de la AWS configuration, la lecture de la AWS configuration pour récupérer la configuration d'Alarm Manager et la création des alarmes Amazon CloudWatch nécessaires.

La `AWSManagedServices_AlarmManagerPermissionsBoundary` politique est attachée au rôle `AWSServiceRoleForManagedServices_DetectiveControlsConfig` lié au service. Pour les mises à jour de ce rôle, consultezAccélérez les mises à jour des rôles liés aux services.

Vous pouvez associer cette politique à vos identités IAM.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `AWS Config`— Autorise les autorisations d'évaluer les règles de configuration et de sélectionner la configuration des ressources.
- `AWS AppConfig`— Autorise l'accès à la AlarmManager configuration.
- `Amazon S3`— Autorise l'utilisation de AlarmManager buckets et d'objets.
- `Amazon CloudWatch`— Autorise les autorisations de lire et de placer les alarmes et les métriques AlarmManager gérées.
- `AWS Resource Groups and Tags`— Autorise la lecture des balises de ressources.
- `Amazon EC2`— Autorise la lecture EC2 des ressources Amazon.
- `Amazon Redshift`— Autorise la lecture des instances et des clusters Redshift.
- `Amazon FSx`— Autorise les autorisations nécessaires pour décrire les systèmes de fichiers, les volumes et les balises de ressources.
- `Amazon CloudWatch Synthetics`— Autorise la lecture des ressources Synthetics.
- `Amazon Elastic Kubernetes Service`— Autorise les autorisations pour décrire le cluster Amazon EKS.
- `Amazon ElastiCache`— Autorise les autorisations pour décrire les ressources.

Vous pouvez télécharger le fichier de politique dans ce fichier ZIP : RecommendedPermissionBoundary.zip.

AWS politique gérée : AWSManagedServices_DetectiveControlsConfig _ ServiceRolePolicy

AWS Managed Services (AMS) utilise la politique `AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` AWS gérée. Cette politique AWS gérée est attachée au rôle `AWSServiceRoleForManagedServices_DetectiveControlsConfig` lié au service (voir). Detective contrôle le rôle lié au service pour AMS Accelerate Pour les mises à jour du rôle `AWSServiceRoleForManagedServices_DetectiveControlsConfig` lié au service, consultez. Accélérez les mises à jour des rôles liés aux services

La politique permet au rôle lié au service d'effectuer des actions à votre place.

Vous pouvez associer la ServiceRolePolicy politique AWSManagedServices_DetectiveControlsConfig _ à vos entités IAM.

Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour AMS Accelerate.

Détails de l'autorisation

Cette politique dispose des autorisations suivantes pour permettre à AWS Managed Services Detective Controls de déployer et de configurer toutes les ressources nécessaires.

- `CloudFormation`— Permet à AMS Detective Controls de déployer des CloudFormation piles avec des ressources telles que des compartiments S3, des règles de configuration et un enregistreur de configuration.
- `AWS Config`— Permet à AMS Detective Controls de créer des règles de configuration AMS, de configurer un agrégateur et de baliser les ressources.
- `Amazon S3`— permet à AMS Detective Controls de gérer ses compartiments s3.

Vous pouvez télécharger le fichier de politique JSON dans ce fichier ZIP : DetectiveControlsConfig_ ServiceRolePolicy .zip.

AWS politique gérée : AWSManaged ServicesDeploymentToolkitPolicy

AWS Managed Services (AMS) utilise la politique `AWSManagedServicesDeploymentToolkitPolicy` AWS gérée. Cette politique AWS gérée est attachée au rôle `AWSServiceRoleForAWSManagedServicesDeploymentToolkit` lié au service (voir). Rôle lié au service du kit de déploiement pour AMS Accelerate La politique permet au rôle lié au service d'effectuer des actions à votre place. Vous ne pouvez pas attacher cette politique à vos entités IAM. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour AMS Accelerate.

Pour les mises à jour du rôle `AWSServiceRoleForManagedServicesDeploymentToolkitPolicy` lié au service, consultez. Accélérez les mises à jour des rôles liés aux services

Détails de l’autorisation

Cette politique dispose des autorisations suivantes pour permettre à AWS Managed Services Detective Controls de déployer et de configurer toutes les ressources nécessaires.

- `CloudFormation`— Permet au kit de déploiement AMS de déployer des piles CFN avec les ressources S3 requises par le CDK.

- `Amazon S3`— permet à AMS Deployment Toolkit de gérer ses compartiments S3.
- `Elastic Container Registry`— permet à AMS Deployment Toolkit de gérer son référentiel ECR qui est utilisé pour déployer les actifs nécessaires aux applications AMS CDK.

Vous pouvez télécharger le fichier de politique JSON dans ce fichier ZIP : AWSManagedServicesDeploymentToolkitPolicy.zip.

AWS politique gérée : AWSManagedServices_EventsServiceRolePolicy

AWS Managed Services (AMS) utilise la politique gérée par `AWSManagedServices_EventsServiceRolePolicy` AWS. Cette politique AWS gérée est attachée au rôle lié au `AWSServiceRoleForManagedServices_Eventsservice`. La politique permet au rôle lié au service d'effectuer des actions à votre place. Vous ne pouvez pas attacher cette politique à vos entités IAM. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour AMS Accelerate.

Pour les mises à jour du rôle `AWSServiceRoleForManagedServices_Events` lié au service, consultez. Accélérez les mises à jour des rôles liés aux services

Détails de l’autorisation

Cette politique comporte les autorisations suivantes pour permettre à Amazon de transmettre EventBridge à AWS Managed Services les informations relatives au changement d'état des alarmes depuis votre compte.

- `events`— Permet à Accelerate de créer une règle EventBridge gérée par Amazon. Cette règle est l'infrastructure dont vous avez besoin Compte AWS pour transmettre les informations de changement d'état des alarmes de votre compte à AWS Managed Services.

Vous pouvez télécharger le fichier de politique JSON dans ce fichier ZIP : EventsServiceRolePolicy.zip.

AWS politique gérée : AWSManagedServices_ContactsServiceRolePolicy

AWS Managed Services (AMS) utilise la politique gérée par `AWSManagedServices_ContactsServiceRolePolicy` AWS. Cette politique AWS gérée est attachée au rôle `AWSServiceRoleForManagedServices_Contacts` lié au service (voir). Création d'un reflex à contacts pour AMS Accelerate Cette politique permet à l'AMS Contacts SLR

de consulter vos balises de ressources, ainsi que leurs valeurs, sur les ressources AWS. Vous ne pouvez pas attacher cette politique à vos entités IAM. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour AMS Accelerate.

> **Important**
>
> Ne stockez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans des balises. AMS utilise des balises pour vous fournir des services d'administration. Les balises ne sont pas destinées à être utilisées pour des données privées ou sensibles.

Pour les mises à jour du rôle `AWSServiceRoleForManagedServices_Contacts` lié au service, consultez. Accélérez les mises à jour des rôles liés aux services

Détails de l'autorisation

Cette politique dispose des autorisations suivantes pour permettre au Contacts SLR de lire vos balises de ressources afin de récupérer les informations de contact des ressources que vous avez configurées à l'avance.

- `IAM`— Permet au service Contacts de consulter les balises associées aux rôles IAM et aux utilisateurs IAM.
- `Amazon EC2`— Permet au service Contacts de consulter les tags des EC2 ressources Amazon.
- `Amazon S3`— Permet au service Contacts de consulter les balises figurant sur les compartiments Amazon S3. Cette action utilise une condition pour garantir qu'AMS accède aux balises de votre bucket à l'aide de l'en-tête d'autorisation HTTP, du protocole de signature SigV4 et du protocole HTTPS avec TLS 1.2 ou supérieur. Pour plus d'informations, consultez Méthodes d'authentification et Clés de politique d'authentification spécifiques à Amazon S3 Signature version 4.
- `Tag`— Permet au service Contacts de consulter les tags d'autres AWS ressources.

- « iam : ListRoleTags », « iam : ListUserTags », « tag : GetResources », « tag : », GetTagKeys « tag : », GetTagValues « ec2 : «, DescribeTags « s3 : » GetBucketTagging

Vous pouvez télécharger le fichier de politique JSON dans ce fichier ZIP : ContactsServicePolicy.zip.

Accélérez les mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées pour Accelerate depuis que ce service a commencé à suivre ces modifications.

Modification	Description	Date

Politique mise à jour — Boîte à outils de déploiement	• Ces nouvelles autorisations ont été ajoutées pour la ressource `arn:aws:ecr:*:*:repository/ams-cdktoolkit*` :
	`ecr:BatchGetRepositoryScanningConfiguration`
	`ecr:PutImageScanningConfiguration`
		4 avril 2024

Politique mise à jour — Boîte à outils de déploiement	• Ces nouvelles autorisations ont été ajoutées pour la ressource `arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*` :
	`cloudformation:DeleteChangeSet`
	`cloudformation:DescribeStackEvents`
	`cloudformation:GetTemplate`
	`cloudformation:TagResource`
	`cloudformation:UntagResource`
	• Ces nouvelles autorisations ont été ajoutées pour la ressource `arn:aws:ecr:*:*:repository/ams-cdktoolkit*` :
	`ecr:CreateRepository`
	`ecr:DeleteLifecyclePolicy`
	`ecr:DeleteRepository`
	`ecr:DeleteRepositoryPolicy`
	`ecr:DescribeRepositories`
	`ecr:GetLifecyclePolicy`
	`ecr:ListTagsForResource`
	`ecr:PutImageTagMutability`
	`ecr:PutLifecyclePolicy`
		9 mai 2023

Modification	Description	Date

	<pre>ecr:SetRepositoryPolicy
	ecr:TagResource
	ecr:UntagResource</pre>
	• En outre, certaines actions existantes comportant un caractère générique ont été réduites à des actions individuelles :
	<pre>- s3:DeleteObject*
	
	+ s3:DeleteObject
	+ s3:DeleteObjectTagging
	+ s3:DeleteObjectVersion
	+ s3:DeleteObjectVersionTagging
	
	- s3:GetObject*
	+ s3:GetObject
	+ s3:GetObjectAcl
	+ s3:GetObjectAttributes
	+ s3:GetObjectLegalHold
	+ s3:GetObjectRetention
	+ s3:GetObjectTagging
	+ s3:GetObjectVersion
	+ s3:GetObjectVersionAcl
	+ s3:GetObjectVersionAttributes
	+ s3:GetObjectVersionForReplication
	+ s3:GetObjectVersionTagging
	+ s3:GetObjectVersionTorrent
	
	- cloudformation:UpdateTermination*
	+ cloudformation:UpdateTerminationProt
	ection</pre>	

Politique mise à jour — Detective Controls	• Les CloudFormation actions ont été précisées après confirmation auprès de l'équipe chargée de la sécurité et de l'accès • Les actions Lambda ont été supprimées de la politique car elles n'ont aucun impact sur l'embarquement onboarding/off	10 avril 2023

Modification	Description	Date
Politique mise à jour — Detective Controls	L'`ListAttachedRolePolicies` action est supprimée de la politique. L'action avait Resource comme caractère générique (*). Comme « liste » est une action non mutative, elle a accès à toutes les ressources et le caractère générique n'est pas autorisé.	28 mars 2023
Politique mise à jour — Detective Controls	Mise à jour de la politique et ajout de la politique de limites des autorisations.	21 mars 2023
Nouvelle politique — Service des contacts	Accelerate a ajouté une nouvelle politique permettant de consulter les informations de contact de votre compte à partir de vos balises de ressources. Accelerate a ajouté une nouvelle politique permettant de lire vos balises de ressources afin de récupérer les informations de contact des ressources que vous avez définies à l'avance.	16 février 2023
Nouvelle politique — Service des événements	Accelerate a ajouté une nouvelle politique pour transmettre à AWS Managed Services les informations relatives au changement d'état des alarmes depuis votre compte. Accorde les rôles IAM créés dans le cadre des Comment fonctionne Alarm Manager autorisations pour créer une règle EventBridge gérée par Amazon requise.	07 février 2023
Politique mise à jour — Boîte à outils de déploiement	Ajout d'autorisations S3 pour permettre aux clients de quitter Accelerate pour quitter Accelerate.	30 janvier 2023
Nouvelle politique — Detective Controls	Permet au rôle lié au service d'effectuer des Detective contrôle le rôle lié au service pour AMS Accelerate actions vous permettant de déployer des contrôles de détection Accelerate.	19 décembre 2022

Modification	Description	Date
Nouvelle politique — Alarm Manager	Accelerate a ajouté une nouvelle politique pour autoriser les autorisations nécessaires à l'exécution des tâches du gestionnaire d'alarmes. Accorde aux rôles IAM créés dans le cadre des Comment fonctionne Alarm Manager autorisations leur permettant d'effectuer des opérations telles que l'évaluation de la AWS configuration, la lecture de la AWS configuration pour récupérer la configuration du gestionnaire d'alarmes, la création des alarmes Amazon CloudWatch nécessaires.	30 novembre 2022
Accélérez le suivi des modifications entamées	Accélérez le suivi initial des modifications apportées AWS à ses politiques gérées.	30 novembre 2022
Nouvelle politique — Boîte à outils de déploiement	Accelerate a ajouté cette politique pour les tâches de déploiement. Accorde au rôle lié au service AWSServiceRoleForAWSManagedServicesDeploymentToolkitles autorisations nécessaires pour accéder aux buckets et stacks Amazon S3 liés au déploiement et les mettre à jour. AWS CloudFormation	9 juin 2022

Protection des données dans Accelerate

AMS Accelerate utilise des outils natifs Services AWS tels qu'Amazon GuardDuty, Amazon Macie (en option) et d'autres outils et processus internes propriétaires pour surveiller en permanence vos comptes gérés. Après le déclenchement d'une alarme, AMS Accelerate assume la responsabilité du triage initial et de la réponse à l'alarme. Les processus de réponse AMS sont basés sur les normes du NIST. AMS Accelerate teste régulièrement les processus de réponse à l'aide de la simulation de réponse aux incidents de sécurité avec vous afin d'aligner votre flux de travail sur les programmes de réponse de sécurité existants des clients.

Lorsqu'AMS Accelerate détecte une violation, ou une menace imminente de violation, de vos politiques de AWS sécurité, Accelerate collecte des informations, y compris les ressources concernées et toute modification liée à la configuration. AMS Accelerate fournit une follow-the-sun assistance 24 heures sur 24, 7 jours sur 7 et 365 jours par an avec des opérateurs dédiés qui examinent et étudient activement les tableaux de bord de surveillance, les files d'attente d'incidents et les demandes de service sur l'ensemble de vos comptes gérés. Accelerate examine les résultats avec des experts en sécurité interne afin d'analyser l'activité et de vous informer par le biais des contacts d'escalade de sécurité répertoriés dans votre compte.

Sur la base des résultats, Accelerate communique avec vous de manière proactive. Si vous constatez que l'activité est non autorisée ou suspecte, AMS travaille avec vous pour enquêter et corriger ou contenir le problème. Certains types de résultats générés par vous GuardDuty obligent à confirmer l'impact avant qu'Accelerate ne prenne des mesures. Par exemple, le type de GuardDuty recherche UnauthorizedAccessIAMUser:/ ConsoleLogin indique que l'un de vos utilisateurs s'est connecté depuis un emplacement inhabituel ; AMS vous avertit et vous demande de revoir le résultat pour confirmer si ce comportement est légitime.

Surveillez avec Amazon Macie

AMS Accelerate prend en charge, et c'est une bonne pratique d'utiliser, Amazon Macie pour détecter une liste importante et complète de données sensibles, telles que des informations de santé personnelles (PHI), des informations personnelles identifiables (PII) et des données financières.

Vous pouvez configurer Macie pour qu'il s'exécute régulièrement sur n'importe quel compartiment Amazon S3. Cela automatise l'évaluation des objets nouveaux ou modifiés dans un bucket au fil du temps. Au fur et à mesure que des résultats de sécurité sont générés, AMS vous en informe et travaille avec vous pour y remédier si nécessaire.

Pour plus d'informations, consultez Analyser les résultats d'Amazon Macie.

Moniteur avec GuardDuty

GuardDuty est un service de surveillance continue de la sécurité qui utilise des flux de renseignements sur les menaces, tels que des listes d'adresses IP et de domaines malveillants, et l'apprentissage automatique pour identifier les activités inattendues, potentiellement non autorisées et malveillantes au sein de votre AWS environnement. Cela peut inclure des problèmes tels que l'augmentation des privilèges, l'utilisation d'informations d'identification exposées ou la communication avec des adresses IP ou des domaines malveillants. GuardDuty surveille le comportement Compte AWS d'accès pour détecter les signes de compromission, tels que les

déploiements d'infrastructure non autorisés, les instances déployées dans une AWS région que vous n'avez jamais utilisée. GuardDuty détecte également les appels d'API inhabituels, tels qu'une modification de la politique de mot de passe visant à réduire la solidité du mot de passe. Pour plus d'informations, consultez le Guide de l'utilisateur GuardDuty .

Pour consulter et analyser vos GuardDuty résultats, procédez comme suit :

1. Ouvrez la GuardDuty console à l'adresse https://console.aws.amazon.com/guardduty/.
2. Choisissez Conclusions, puis sélectionnez une constatation spécifique pour afficher les détails. Les détails de chaque constatation diffèrent selon le type de découverte, les ressources impliquées et la nature de l'activité.

Pour plus d'informations sur les champs de recherche disponibles, consultez la section Détails de la GuardDuty recherche.

Utiliser les règles de GuardDuty suppression pour filtrer les résultats

Une règle de suppression est un ensemble de critères qui consiste en un attribut de filtre associé à une valeur. Vous pouvez utiliser des règles de suppression pour filtrer les résultats de faible valeur auxquels vous n'avez pas l'intention de donner suite, tels que les résultats faussement positifs ou les activités connues. Le filtrage de vos résultats permet d'identifier plus facilement les menaces de sécurité susceptibles d'avoir le plus d'impact sur votre environnement.

Pour filtrer les résultats, les règles de suppression archivent automatiquement les nouveaux résultats correspondant aux critères que vous avez spécifiés. Les résultats archivés ne sont pas envoyés à AWS Security Hub, Amazon S3 ou CloudTrail Events. Les filtres de suppression réduisent donc les données inexploitables si vous consultez GuardDuty les résultats via Security Hub ou une application d'alerte et de billetterie SIEM tierce.

AMS dispose d'un ensemble défini de critères pour identifier les règles de suppression pour vos comptes gérés. Lorsqu'un compte géré répond à ces critères, AMS applique les filtres et vous adresse une demande de service (SR) détaillant le filtre de suppression déployé.

Vous pouvez communiquer avec AMS via un SR pour modifier ou annuler les filtres de suppression.

Afficher les résultats archivés

GuardDuty continue de générer des résultats même lorsque ceux-ci correspondent à vos règles de suppression. Les résultats supprimés sont marqués comme archivés. GuardDuty conserve les résultats archivés pendant 90 jours. Vous pouvez consulter les résultats archivés dans la GuardDuty

console pendant ces 90 jours en sélectionnant Archivé dans le tableau des résultats. Vous pouvez également consulter les résultats archivés via l' GuardDuty API en utilisant l'ListFindingsAPI avec un FindingCriteria de service.archived égal à true.

Cas d'utilisation courants des règles de suppression

Les types de recherche suivants présentent des cas d'utilisation courants pour appliquer des règles de suppression.

- Recon : EC2 /Portscan : utilisez une règle de suppression pour archiver automatiquement les résultats lorsque vous utilisez un scanner de vulnérabilités autorisé.
- UnauthorizedAccess:EC2/SSHBruteForce : utilisez une règle de suppression pour archiver automatiquement les résultats lorsqu'ils ciblent des instances de bastion.
- Recon :EC2/PortProbeUnprotectedPort: Utilisez une règle de suppression pour archiver automatiquement les résultats lorsqu'ils ciblent des instances exposées intentionnellement.

Surveillez avec le pare-feu DNS Amazon Route 53 Resolver

Amazon Route 53 Resolver répond de manière récursive aux requêtes DNS provenant AWS des ressources relatives aux archives publiques, aux noms DNS spécifiques à Amazon VPC et aux zones hébergées privées Amazon Route 53. Il est disponible par défaut dans tous les domaines. VPCs Avec Route 53 Resolver DNS Firewall, vous pouvez filtrer et réguler le trafic DNS sortant pour votre cloud privé virtuel (VPC). Pour ce faire, créez des collections réutilisables de règles de filtrage dans les groupes de règles de pare-feu DNS, associez les groupes de règles à votre VPC, puis contrôlez l'activité dans les journaux et les métriques du pare-feu DNS. En fonction de l'activité, vous pouvez ajuster le comportement du pare-feu DNS en conséquence. Pour plus d'informations, voir Utilisation du pare-feu DNS pour filtrer le trafic DNS sortant.

Pour afficher et gérer la configuration de votre pare-feu DNS Route 53 Resolver, suivez la procédure suivante :

1. Connectez-vous à la console Amazon VPC AWS Management Console et ouvrez-la à l'adresse. https://console.aws.amazon.com/vpc/
2. Sous Pare-feu DNS, sélectionnez Groupes de règles.
3. Vérifiez, modifiez ou supprimez votre configuration existante, ou créez un nouveau groupe de règles. Pour plus d'informations, consultez Comment fonctionne le pare-feu DNS Route 53 Resolver.

Surveillance et sécurité du pare-feu DNS Amazon Route 53 Resolver

Le pare-feu DNS Amazon Route 53 utilise les concepts d'associations de règles, d'action des règles et de priorité d'évaluation des règles. Une liste de domaines est un ensemble réutilisable de spécifications de domaine que vous utilisez dans une règle de pare-feu DNS, à l'intérieur d'un groupe de règles. Lorsque vous associez un groupe de règles à un VPC, le pare-feu DNS compare vos requêtes DNS aux listes de domaines qui sont utilisées dans les règles. Si le pare-feu DNS trouve une correspondance, il gère la requête DNS conformément à l'action de la règle correspondante. Pour plus d'informations sur les groupes de règles et les règles, consultez la section Groupes de règles et règles du pare-feu DNS.

Les listes de domaines se répartissent en deux catégories principales :

- Des listes de domaines gérées, AWS créées et mises à jour pour vous.
- Vos propres listes de domaines, que vous créez et gérez.

Les groupes de règles sont évalués en fonction de leur indice de priorité d'association.

Par défaut, AMS déploie une configuration de base composée des règles et groupes de règles suivants :

- Un groupe de règles nommé`DefaultSecurityMonitoringRule`. Le groupe de règles possède la priorité d'association la plus élevée disponible au moment de la création pour chaque VPC existant dans chaque VPC activé. Région AWS
- Une règle nommée `DefaultSecurityMonitoringRule` avec la priorité 1 au sein du groupe de `DefaultSecurityMonitoringRule` règles, utilisant la liste des domaines `AWSManagedDomainsAggregateThreatList` gérés avec l'action ALERT.

Si vous avez une configuration existante, la configuration de base est déployée avec une priorité inférieure à celle de votre configuration existante. Votre configuration existante est la configuration par défaut. Vous utilisez la configuration de base AMS comme fourre-tout si votre configuration existante ne fournit pas d'instructions prioritaires sur la manière de gérer la résolution des requêtes. Pour modifier ou supprimer la configuration de référence, effectuez l'une des opérations suivantes :

- Contactez votre responsable de prestation de services cloud (CSDM) ou votre architecte cloud (CA).
- Créez une demande de service.

Chiffrement des données dans AMS Accelerate

AMS Accelerate en utilise plusieurs Services AWS pour le chiffrement des données.

Amazon Simple Storage Service propose plusieurs options de chiffrement d'objets qui protègent les données en transit et au repos. Le chiffrement côté serveur chiffre vos objets avant de les enregistrer sur les disques des centres de données, puis les déchiffre lorsque vous téléchargez les objets. Tant que vous authentifiez votre demande et que vous avez des autorisations d'accès, il n'y a aucune différence dans la manière dont vous accédez aux objets chiffrés ou déchiffrés. Pour plus d'informations, consultez la section Protection des données dans Amazon S3.

AWS Identity and Access Management dans AMS Accelerate

AWS Identity and Access Management est un service Web qui vous permet de contrôler en toute sécurité l'accès aux AWS ressources. Vous pouvez utiliser IAM pour contrôler les personnes qui s'authentifient (sont connectées) et sont autorisées (disposent d'autorisations) à utiliser des ressources. Lors de l'intégration d'AMS Accelerate, vous êtes chargé de créer des rôles d'administrateur IAM entre comptes au sein de chacun de vos comptes gérés.

Dans AMS Accelerate, vous êtes responsable de la gestion de l'accès à vos ressources Comptes AWS et à leurs ressources sous-jacentes, telles que les solutions de gestion des accès, les politiques d'accès et les processus associés. Cela signifie que vous gérez le cycle de vie de vos utilisateurs, les autorisations dans les services d'annuaire et le système d'authentification fédérée, pour accéder à la AWS console ou AWS APIs. Pour vous aider à gérer votre solution d'accès, AMS Accelerate déploie des AWS Config règles qui détectent les erreurs de configuration courantes de l'IAM et envoie des notifications de correction. Pour en savoir plus, consultez Règles gérées AWS Config.

Authentification avec des identités dans AMS Accelerate

AMS utilise des rôles IAM, qui sont un type d'identité IAM. Un rôle IAM est similaire à un utilisateur, dans la mesure où il s'agit d'une identité dotée de politiques d'autorisation qui déterminent ce que l'identité peut et ne peut pas faire. AWS Cependant, aucun identifiant n'est associé à un rôle et, au lieu d'être associé de manière unique à une seule personne, il peut être assumé par tous ceux qui en ont besoin. Un utilisateur IAM peut endosser un rôle pour accepter différentes autorisations temporaires concernant un tâche spécifique.

Les rôles d'accès sont contrôlés par l'appartenance à un groupe interne, qui est administré et révisé périodiquement par la direction des opérations. AMS utilise les rôles IAM suivants.

> **Note**
>
> Les rôles d'accès AMS permettent aux opérateurs AMS d'accéder à vos ressources pour fournir des fonctionnalités AMS (voirService description (Description du service)). La modification de ces rôles peut entraver notre capacité à fournir ces capacités. Si vous devez modifier les rôles d'accès AMS, consultez votre architecte cloud.

Nom de rôle	Description
Utilisé par (entité) : AMS Access Service uniquement	
ams-access-management	Déployé manuellement par vos soins lors de l'intégration. Supposé uniquement par AMS Access pour déployer ou mettre à jour les rôles d'accès. Reste dans votre compte après l'intégration pour toute future mise à jour des rôles d'accès.
Utilisé par (entité) : AMS Operations	
ams-access-admin-operations	Ce rôle dispose des autorisations administr atives nécessaires pour opérer dans les comptes, mais pas pour lire, écrire ou supprimer le contenu client dans les AWS services couramment utilisés comme magasins de données, tels qu'Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift et Amazon. ElastiCache Seules quelques personnes sélectionnées dans le cadre de l'AMS peuvent assumer ce rôle.
ams-access-operations	Ce rôle AMS Operations est autorisé à effectuer des tâches administratives dans vos comptes. Ce rôle ne dispose pas d'autoris ations de lecture, d'écriture ou de suppressi on du contenu client dans les AWS services

Nom de rôle	Description
	couramment utilisés comme magasins de données, tels qu'Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift et Amazon. ElastiCache Les autorisations permettant d'effectuer des opérations d' AWS Identity and Access Management écriture sont également exclues de ce rôle.
ams-access-read-only	Ce rôle en lecture seule AMS est limité aux autorisations en lecture seule de votre compte AMS. Les autorisations de lecture du contenu client dans les AWS services couramment utilisés comme magasins de données, tels qu'Amazon S3, Amazon RDS, DynamoDB, Amazon Redshift, etc. ne sont pas accordées par ElastiCache ce rôle.
Utilisé par (entité) : AMS Operations et AMS Services	
ams_ssm_automation_role	Supposé par AWS Systems Manager exécuter les documents SSM Automation sur votre compte.
ams_ssm_automation_role	
Utilisé par (entité) : AMS Security	

Nom de rôle	Description
ams-access-security-analyst	Ce rôle de sécurité AMS est autorisé dans votre compte AMS à effectuer une surveillance dédiée des alertes de sécurité et à la gestion des incidents de sécurité. Seules quelques personnes sélectionnées d'AMS Security peuvent assumer ce rôle. Les autorisations de lecture du contenu client dans les AWS services couramment utilisés comme magasins de données, tels qu'Amazon S3, Amazon RDS, Amazon DynamoDB, Amazon Redshift, ne sont pas ElastiCache accordées par ce rôle.
ams-access-security-analyst-lecture seule	Ce rôle de sécurité AMS est limité aux autorisations en lecture seule de votre compte AMS pour effectuer une surveillance dédiée des alertes de sécurité et une gestion des incidents de sécurité. Les autorisations de lecture du contenu client dans les AWS services couramment utilisés comme magasins de données, tels qu'Amazon S3, Amazon RDS, Amazon DynamoDB, Amazon Redshift, ne sont pas ElastiCache accordées par ce rôle.
Utilisé par (entité) : AWS Services	
ams-access-admin	Ce rôle d'administrateur AMS dispose de toutes les autorisations nécessaires pour opérer sur des comptes sans restrictions. Seuls les services internes d'AMS (avec une politique de session limitée) peuvent assumer le rôle d'administrateur.

Nom de rôle	Description
ams-opscenter-eventbridge-role	Supposé par Amazon EventBridge AWS Systems Manager OpsItems comme étant créé dans le cadre d'un flux de travail de AWS Config Rules correction spécifique à AMS.
AMSOSConfigurationCustomerInstanceRole	Ce rôle IAM est appliqué à vos EC2 instances Amazon lorsque le service de configuration du système d'exploitation AMS découvre que les politiques IAM requises sont manquantes. Il permet à vos EC2 instances Amazon d'interag ir avec AWS Systems Manager Amazon et CloudWatch les EventBridge services Amazon. Il a également joint la politique gérée personnal isée AMS pour permettre l'accès RDP à vos instances Windows.
mc-patch-glue-service-rôle	Supposé par le flux de travail AWS Glue ETL pour effectuer la transformation des données et les préparer pour le générateur de rapports AMS Patch.
Utilisé par (entité) : AMS Service	
ams-alarm-manager- AWSManaged ServicesA larmManagerDe - <8-digit hash>	Supposé par l'infrastructure du gestionnaire d'alarmes AMS au sein de votre compte AMS pour effectuer une AWS Config Rules évaluatio n en vue d'un nouveau AWS AppConfig déploiement.
ams-alarm-manager- AWSManaged ServicesA larmManagerRe - <8-digit hash>	Supposée par l'infrastructure de correction du gestionnaire d'alarmes AMS au sein de votre compte AMS pour permettre la création ou la suppression d'alarmes à des fins de correction.

Nom de rôle	Description
ams-alarm-manager- AWSManaged ServicesAlarmManager SS- <8-digit hash>	Supposé par AWS Systems Manager appeler le service de correction du gestionnaire d'alarmes AMS dans votre compte AMS.
ams-alarm-manager- AWSManaged ServicesAlarmManagerTr - <8-digit hash>	Supposé par l'infrastructure du gestionnaire d'alarmes AMS au sein de votre AWS compte pour effectuer une AWS Config Rules évaluation AMS périodique.
ams-alarm-manager- AWSManaged ServicesAlarmManagerVa - <8-digit hash>	Supposée par l'infrastructure du gestionnaire d'alarmes AMS au sein de votre compte AMS pour garantir que les alarmes requises existent dans le AWS compte.
ams-backup-iam-role	Ce rôle est utilisé pour fonctionner AWS Backup au sein de vos comptes.
surveillance AMS-- AWSManaged ServicesLogGroupLimitLamb <8-digit hash>	Supposé par l'infrastructure de journalisation et de surveillance AMS de votre compte AMS pour évaluer la limite CloudWatch des groupes Amazon Logs et la comparer aux quotas de service.
surveillance des ondes- AWSManaged Services RDSMonitoring RDSE- <8-digit hash>	Supposé par l'infrastructure de journalisation et de surveillance AMS de votre compte AMS pour transférer les événements Amazon RDS vers Amazon CloudWatch Events.
surveillance AMS-- AWSManaged ServicesRedshiftMonitorin <8-digit hash>	Supposé par l'infrastructure de journalisation et de surveillance AMS de votre compte AMS pour transférer les événements Amazon Redshift (CreateCluster et DeleteCuster) vers Amazon CloudWatch Events.

Nom de rôle	Description
ams-monitoring-infrastruc- AWSManaged ServicesMonito - <8-digit hash>	L'infrastructure AMS Logging & Monitoring de votre compte AMS est censée publier des messages sur Amazon Simple Notification Service afin de valider que le compte fournit toutes les données nécessaires.
ams-opscenter-role	Supposé par le système de gestion des notifications AMS de votre compte AMS AWS Systems Manager OpsItems pour gérer les alertes de votre compte.
ams-opsitem-autoexecution-role	Supposé par le système de gestion des notifications AMS pour gérer la correction automatique à l'aide de documents SSM pour surveiller les alertes liées aux ressources de votre compte.
ams-patch-infrastructure-amspatchconfigrulero leC1- <8-digit hash>	Supposé par AWS Config pour évaluer les ressources des correctifs AMS et détecter la dérive dans ses AWS CloudFormation piles.
ams-patch-infrastructure-amspatchcwruleopsite mams- <8-digit hash>	Supposé par Amazon EventBridge pour être créé en cas AWS Systems Manager OpsItems d'échec des correctifs.
ams-patch-infrastructure-amspatchser vicebusamspat- <8-digit hash>	Supposé par Amazon EventBridge pour envoyer un événement au bus d'événeme nts AMS Patch Orchestrator pour les notificat ions de modification de l'état de AWS Systems Manager Maintenance Windows.
ams-patch-reporting-infra-amspatchreportingco nfigr- <8-digit hash>	Supposé par AWS Config pour évaluer les ressources de reporting d'AMS Patch et détecter la dérive dans ses AWS CloudForm ation piles.

Nom de rôle	Description
ams-resource-tagger- AWSManaged ServicesResourceTagg - <8-digit hash>	Supposé par l'infrastructure AMS Resource Tagger au sein de votre compte AMS pour effectuer une AWS Config Rules évaluation lors d'un nouveau AWS AppConfig déploiement.
ams-resource-tagger- AWSManaged ServicesResourceTagg - <8-digit hash>	Supposé par l'infrastructure AMS Resource Tagger au sein de votre compte AMS pour valider l'existence des AWS balises requises pour les ressources gérées.
ams-resource-tagger- AWSManaged ServicesResourceTagg - <8-digit hash>	Supposé par AWS Systems Manager invoquer le flux de travail de correction AMS Resource Tagger dans votre compte AMS.
ams-resource-tagger- AWSManaged ServicesResourceTagg - <8-digit hash>	Supposée par l'infrastructure de correction AMS Resource Tagger au sein de votre compte AMS pour créer ou supprimer des AWS balises pour les ressources gérées.
ams-resource-tagger- AWSManaged ServicesResourceTagg - <8-digit hash>	Supposé par l'infrastructure AMS Resource Tagger de votre AWS compte pour effectuer une évaluation périodique des règles de configuration AMS.
ams_os_configuration_event_rule_role- <AWS Region>	Supposé par Amazon EventBridge pour transférer les événements de votre compte au service de configuration du système d'exploitation AMS EventBus dans la bonne région.
mc-patch-reporting-service	Supposé par l'agrégateur de données de patch et le générateur de rapports AMS.

> **Note**
>
> Il s'agit du modèle du ams-access-management rôle. Il s'agit de la pile que les architectes du cloud (CAs) déploient manuellement dans votre compte lors de l'intégration : management-role.yaml.
> Il s'agit du modèle pour les différents rôles et niveaux d'accès : ams-access-read-only,, ams-access-operations ams-access-admin-operations, ams-access-admin : accelerate-roles.yaml.

Pour en savoir plus sur les identifiants AWS Cloud Development Kit (AWS CDK) (AWS CDK), y compris les hachages, consultez Unique. IDs

Les services de fonctionnalités AMS Accelerate ams-access-adminjouent le rôle d'accès programmatique au compte, mais avec une politique de session définie pour le service de fonctionnalités concerné (par exemple, correctif, sauvegarde, surveillance, etc.).

AMS Accelerate suit les meilleures pratiques du secteur pour respecter et maintenir l'éligibilité en matière de conformité. L'accès à votre compte AMS Accelerate est enregistré CloudTrail et peut également être consulté par le biais du suivi des modifications. Pour plus d'informations sur les requêtes que vous pouvez utiliser pour obtenir ces informations, consultezSuivi des modifications apportées à vos comptes AMS Accelerate.

Gestion des accès à l’aide de politiques

Diverses équipes de support d'AMS Accelerate, telles que les ingénieurs d'exploitation, les architectes cloud et les responsables de la prestation de services cloud (CSDMs), ont parfois besoin d'accéder à vos comptes pour répondre aux demandes de service et aux incidents. Leur accès est régi par un service d'accès AMS interne qui applique des contrôles, tels que la justification commerciale, les demandes de service, les éléments opérationnels et les dossiers de support. L'accès par défaut est en lecture seule, et tous les accès sont suivis et enregistrés ; voir également. Suivi des modifications apportées à vos comptes AMS Accelerate

Validation des ressources IAM

Le système d'accès AMS Accelerate assume régulièrement des rôles dans vos comptes (au moins toutes les 24 heures) et vérifie que toutes nos ressources IAM sont conformes aux attentes.

Afin de protéger vos comptes, AMS Accelerate dispose d'un « canari » qui surveille et émet des alertes concernant la présence et le statut des rôles IAM, ainsi que les politiques associées,

mentionnées ci-dessus. Régulièrement, le Canary assume le ams-access-read-onlyrôle CloudFormation et lance des appels d'API IAM vers vos comptes. Le canari évalue l'état des rôles d'accès AMS Accelerate pour s'assurer qu'ils ne sont toujours pas modifiés et. up-to-date Cette activité crée CloudTrail des connexions dans le compte.

Le nom de session AWS Security Token Service (AWS STS) du canary est AMS-Access-Roles-Auditor- {uuid4 ()} comme indiqué dans et les appels d'API suivants ont lieu : CloudTrail

- Appels d'API Cloud Formation : `describe_stacks()`
- Appels d'API IAM :
  - `get_role()`
  - `list_attached_role_policies()`
  - `list_role_policies()`
  - `get_policy()`
  - `get_policy_version()`
  - `get_role_policy()`

Réponse aux incidents de sécurité dans AMS

La sécurité est la priorité absolue d'AWS Managed Services (AMS). AMS déploie des ressources et des contrôles dans vos comptes pour les gérer. AWS a un modèle de responsabilité partagée : AWS gère la sécurité du cloud, et vous êtes responsable de la sécurité dans le cloud. AMS protège vos données et vos actifs et contribue à la sécurité de votre AWS infrastructure en utilisant des contrôles de sécurité et une surveillance active des problèmes de sécurité. Ces fonctionnalités vous aident à établir une base de sécurité pour les applications exécutées dans le AWS cloud. AMS collabore avec vous par le biais de Security Incident Response afin d'en évaluer les effets, puis de mettre en œuvre des mesures de confinement et de correction sur la base des recommandations des meilleures pratiques.

Lorsqu'un écart par rapport à la ligne de base se produit, par exemple en raison d'une mauvaise configuration ou d'une modification de facteurs externes, vous devez réagir et enquêter. Pour y parvenir, vous devez comprendre les concepts de base de la réponse aux incidents de sécurité dans votre environnement AMS. Vous devez également comprendre les exigences relatives à la préparation, à la formation et à la formation des équipes cloud avant que des problèmes de sécurité ne surviennent. Il est important de connaître les contrôles et les fonctionnalités que vous pouvez utiliser, de préparer des plans de réponse pour les problèmes de sécurité courants tels que la

compromission d'un compte utilisateur ou l'utilisation abusive de comptes privilégiés, et d'identifier les méthodes de correction qui utilisent l'automatisation pour améliorer la vitesse de réponse et la cohérence. En outre, vous devez comprendre vos exigences réglementaires et de conformité en ce qui concerne l'élaboration d'un programme de réponse aux incidents de sécurité pour répondre à ces exigences.

La réponse aux incidents de sécurité peut être complexe, mais en mettant en œuvre une approche itérative, vous pouvez simplifier le processus et permettre à l'équipe de réponse aux incidents de satisfaire les parties prenantes des actifs en fournissant une détection et une réponse rapides et continues. Dans ce guide, nous vous expliquons la méthodologie utilisée par AMS pour répondre aux incidents, la matrice de responsabilité AMS (RACI), comment vous préparer à un événement de sécurité, comment engager AMS lors d'incidents de sécurité et certains des manuels de réponse aux incidents utilisés par AMS.

Comment fonctionne AMS Security Incident Response

AWS Managed Services s'aligne sur le guide de gestion des incidents de sécurité informatique 800-61 du NIST pour la réponse aux incidents de sécurité. En nous alignant sur cette norme du secteur, nous proposons une approche cohérente de la gestion des événements de sécurité et nous adhérons aux meilleures pratiques en matière de sécurisation et de réponse aux incidents de sécurité dans votre cloud.

Cycle de vie de réponse aux incidents

Lorsque la détection identifie et génère une alerte de sécurité, ou que vous demandez une assistance en matière de sécurité, l'équipe AWS Managed Services Operations veille à ce qu'une enquête soit menée en temps opportun, exécute des automatisations pour effectuer la collecte de données, les triages et les analyses, vous informe de l'analyse, effectue des enquêtes et des activités de confinement, puis publie une analyse des événements.

Les activités de collecte, de triage, d'analyse et de confinement des données effectuées lors de la réponse à un incident varient en fonction du type d'événement de sécurité étudié. Des exemples de flux de travail de réponse aux incidents de sécurité pour certains scénarios figurent à la fin de ce document.

Lors d'incidents, AMS détermine de manière dynamique le bon plan d'action, ce qui peut entraîner la réorganisation ou le contournement des étapes documentées, le cas échéant, afin de garantir le bon résultat.

Préparation

À mesure que le paysage des menaces évolue, AMS continue d'étendre ses capacités de détection et de réponse. Au fur et à mesure que de nouvelles détections sont ajoutées, AMS intègre les alertes issues de ces nouvelles détections dans la plateforme de détection et de réponse. Les intervenants de sécurité AMS sont formés pour enquêter et collaborer avec vous tout au long du cycle de vie de réponse aux incidents de sécurité.

En raison de cette approche de partenariat, il est important que vos équipes chargées de la sécurité et des applications soient prêtes à collaborer avec AMS pour gérer les événements de sécurité au fur et à mesure qu'ils se produisent. Cette documentation explique à quoi s'attendre lors d'un événement de sécurité et vous aide à vous préparer à une intervention rapide en cas d'incident de sécurité.

Cette documentation utilise la définition NIST 800-61 d'un événement comme tout événement observable dans un système ou un réseau et d'un incident comme une violation ou une menace imminente de violation des politiques, des politiques d'utilisation acceptable ou des pratiques de sécurité standard.

Liste de contrôle pour la préparation

Suivez la liste de contrôle suivante avec votre gestionnaire de mise à disposition de solutions cloud (CSDM) AMS et votre architecte cloud AMS (CA) :

- Découvrez quelles charges de travail sont exécutées sur quels comptes.
- Déterminez quelles équipes internes sont responsables des différentes charges de travail et étiquez-les de manière appropriée dans les charges de travail.
- Conservez en interne les coordonnées des autres équipes qui pourraient être nécessaires lors d'une enquête sur un événement de sécurité et pour les décisions relatives au confinement.
- Vérifiez que les contacts de sécurité sont à jour et ajoutés à tous les AWS comptes gérés. Les contacts sont gérés par compte.
- Sachez comment signaler un incident de sécurité à AMS, et familiarisez-vous avec la gravité et les temps de réponse attendus.
- Assurez-vous que lorsque des notifications de sécurité sont reçues, elles sont acheminées vers les personnes et les systèmes appropriés, tels que les téléavertisseurs ou votre centre des opérations de sécurité.
- Découvrez quelles sources de journaux sont à votre disposition, où elles sont stockées dans vos comptes et qui y a accès.

- Découvrez comment utiliser CloudWatch Insights pour interroger les journaux pendant les enquêtes.
- Découvrez les options de confinement qui s'offrent à vous par ressource (IAMEC2, S3, etc.) et les conséquences sur la disponibilité de votre charge de travail en cas de confinement.

Détection

Lors de la gestion de vos AWS comptes, AMS surveille les anomalies dans le comportement des utilisateurs, les activités des comptes et les éventuels événements de sécurité à l'aide des données collectées auprès de sources de détection et de contrôles, notamment Amazon CloudWatch, Amazon GuardDuty, VPC Flow Logs, Amazon Macie AWS Config et les flux internes de Threat Intelligence d'Amazon.

AMS utilise à la fois AWS des services natifs et d'autres technologies de détection pour répondre aux événements de sécurité créés par :

- Types de recherche de conformité de configuration
- GuardDuty Trouver des types
- Types de recherche de Macie
- Événements du pare-feu DNS Amazon Route 53 Resolver
- Événements de sécurité AMS (alarmes de surveillance dans le cloud)

Des résultats supplémentaires sont ajoutés à mesure que les services, les produits et les écosystèmes de menaces évoluent.

Signaler les événements de sécurité à AMS

Signalez un incident via le portail ou le Support centre de support AMS pour informer AMS d'un incident de sécurité ou pour demander une enquête.

Analyser

Une fois qu'un événement de sécurité est identifié et signalé, l'étape suivante consiste à analyser s'il s'agit d'un faux positif ou d'un incident réel. AMS utilise des techniques d'automatisation et d'investigation manuelle pour gérer les événements de sécurité. L'analyse inclut l'examen des journaux provenant de différentes sources de détection, telles que les journaux de trafic réseau, les

journaux d'hôte, les CloudTrail événements, les journaux de AWS service, etc. L'analyse recherche également des modèles qui montrent un comportement anormal par corrélation.

Votre partenariat est nécessaire pour comprendre le contexte propre à l'environnement du compte et pour déterminer ce qui est normal pour votre compte et vos charges de travail. Cela permet à AMS d'identifier une anomalie plus rapidement et d'accélérer la réponse aux incidents.

Gérer les communications d'AMS concernant les événements de sécurité

AMS vous tient informé tout au long de l'enquête en contactant vos contacts de sécurité par le biais d'un ticket d'incident. Votre responsable de prestation de services cloud (CSDM) AMS et votre architecte cloud AMS (CA) sont les points de contact à contacter pour toute communication lors d'une enquête de sécurité en cours.

La communication inclut la notification automatique lorsqu'une alerte de sécurité est générée, l'analyse des communications après les événements, l'établissement de passerelles téléphoniques et la livraison continue d'artefacts tels que des fichiers journaux, un instantané des ressources infectées, et la communication des résultats de l'enquête pendant l'événement de sécurité.

Les champs standard inclus dans les notifications d'alerte de sécurité AMS sont répertoriés ci-dessous. Ces champs vous fournissent des informations qui vous permettent d'acheminer les événements vers les équipes appropriées au sein de votre organisation pour qu'elles y remédient.

- Type de recherche
- Trouver un identifiant (le cas échéant)
- Déterminer la gravité
- Description de la recherche
- Trouver la date et l'heure de création
- AWS ID du compte
- Région (le cas échéant)
- AWS Ressources (IAMuser/role/policy, S3 EC2, EKS)

Des champs supplémentaires sont fournis en fonction du type de recherche. Par exemple, les résultats EKS incluent les détails du pod, du conteneur et du cluster.

Contenir

L'approche d'AMS en matière de confinement repose sur un partenariat avec vous. Vous comprenez votre activité et les impacts sur la charge de travail qui peuvent découler des activités de confinement, telles que l'isolation du réseau, le déprovisionnement des utilisateurs ou des rôles IAM, la reconstruction d'instances, etc.

La prise de décision est un élément essentiel de l'endiguement. Par exemple, arrêtez un système, isolez une ressource du réseau, désactivez l'accès ou mettez fin à des sessions. Ces décisions sont plus faciles à prendre s'il existe des stratégies et des procédures prédéterminées pour contenir l'incident. AMS fournit la stratégie de confinement, puis met en œuvre la solution après avoir pris en compte le risque lié à la mise en œuvre des actions de confinement.

Il existe différentes options de confinement en fonction des ressources analysées. AMS s'attend à ce que plusieurs types de confinement soient déployés simultanément lors d'une enquête sur un incident. Certains de ces exemples incluent :

- Appliquez des règles de protection pour bloquer le trafic non autorisé (groupe de sécurité, NACL, règles WAF, règles SCP, refus de la liste, définition de l'action de signature en quarantaine ou en blocage)
- Isolation des ressources
- Isolement du réseau
- Désactivation des utilisateurs, des rôles et des politiques IAM
- Modification/réduction de l'utilisateur IAM, du privilège de rôle
- Terminer, suspendre ou supprimer des ressources de calcul
- Restreindre l'accès public à la ressource affectée
- Rotation des clés d'accès, des clés API et des mots de passe
- Effacement des informations d'identification divulguées et des informations sensibles

AMS vous encourage à envisager le type de stratégies de confinement pour chaque type d'incident majeur qui correspond à leur propension au risque, avec des critères clairement documentés pour faciliter la prise de décision en cas d'incident. Les critères permettant de déterminer la stratégie appropriée sont notamment les suivants :

- Dommages potentiels aux ressources
- Préservation des preuves

- Indisponibilité du service (par exemple, connectivité réseau, services fournis à des tiers externes)
- Temps et ressources nécessaires à la mise en œuvre de la stratégie
- Efficacité de la stratégie (par exemple, confinement partiel, confinement complet)
- Permanence de la solution (par exemple, décisions relatives à une porte à sens unique ou à une porte bidirectionnelle)
- Durée de la solution (par exemple, solution d'urgence à supprimer dans quatre heures, solution temporaire à supprimer dans deux semaines, solution permanente).
- Appliquez des contrôles de sécurité que vous pouvez activer afin de réduire les risques et de disposer du temps nécessaire pour définir et mettre en œuvre un confinement plus efficace.

La rapidité du confinement étant essentielle, AMS conseille une approche par étapes pour parvenir à un confinement efficient et efficace en élaborant des stratégies à court et à long terme.

Utilisez ce guide pour réfléchir à votre stratégie de confinement qui implique différentes techniques en fonction du type de ressource.

- Stratégie de confinement
  - AMS peut-il identifier l'ampleur de l'incident de sécurité ?
    - Dans l'affirmative, identifiez toutes les ressources (utilisateurs, systèmes, ressources).
    - Si ce n'est pas le cas, étudiez en parallèle avec l'exécution de l'étape suivante sur les ressources identifiées.
  - La ressource peut-elle être isolée ?
    - Si c'est le cas, isolez les ressources affectées.
    - Si ce n'est pas le cas, travaillez avec les propriétaires et les gestionnaires du système pour déterminer les mesures supplémentaires nécessaires pour contenir le problème.
  - Toutes les ressources affectées sont-elles isolées des ressources non touchées ?
    - Dans l'affirmative, passez à l'étape suivante.
    - Si ce n'est pas le cas, continuez à isoler les ressources affectées jusqu'à ce que le confinement à court terme soit réalisé afin d'éviter que l'incident ne s'aggrave davantage.
- Sauvegarde du système
  - Des copies de sauvegarde des systèmes concernés ont-elles été créées pour une analyse plus approfondie ?
  - Les copies médico-légales sont-elles cryptées et stockées dans un endroit sûr ?

- Dans l'affirmative, passez à l'étape suivante.
- Si ce n'est pas le cas, chiffrez les images médico-légales, puis stockez-les dans un endroit sûr pour éviter toute utilisation accidentelle, tout dommage ou toute altération.

Éradiquer

Une fois qu'un incident est maîtrisé, il peut être nécessaire de l'éradiquer pour éliminer complètement les sources de menace afin de sécuriser le système avant de passer à l'étape de restauration suivante. Les mesures d'éradication peuvent inclure la suppression des logiciels malveillants et la suppression des comptes utilisateurs compromis, ainsi que l'identification et l'atténuation de toutes les vulnérabilités exploitées. Lors de l'éradication, il est important d'identifier tous les comptes, ressources et instances concernés au sein de l'environnement afin de pouvoir y remédier.

Il est recommandé que l'éradication et le rétablissement soient effectués par étapes afin que les étapes d'assainissement soient hiérarchisées. Pour les incidents de grande envergure, le rétablissement peut prendre des mois. L'objectif des premières phases doit être d'accroître la sécurité globale grâce à des modifications de grande valeur relativement rapides (quelques jours à plusieurs semaines) afin de prévenir de futurs incidents. Les phases ultérieures doivent se concentrer sur les changements à long terme (par exemple, les changements d'infrastructure) et sur le travail continu visant à assurer la sécurité de l'entreprise autant que possible.

Pour certains incidents, l'éradication n'est pas nécessaire ou est effectuée pendant le rétablissement.

Éléments à prendre en compte :

- Est-il possible de recréer une image du système puis de le renforcer à l'aide de correctifs ou d'autres contre-mesures pour prévenir ou réduire le risque d'attaques ?
- Tous les malwares et autres artefacts laissés par les attaquants ont-ils été supprimés et les systèmes affectés sont-ils renforcés contre de nouvelles attaques ?

Récupération

AMS collabore avec vous pour rétablir le fonctionnement normal des systèmes, vérifier qu'ils fonctionnent normalement et (le cas échéant) corriger les vulnérabilités afin d'éviter des incidents similaires.

Éléments à prendre en compte :

- Le ou les systèmes concernés ont-ils été corrigés et renforcés contre la récente attaque et les attaques futures possibles ?
- À quel jour et à quelle heure est-il possible de remettre en production les systèmes concernés ?
- Quels outils utiliserez-vous pour tester, surveiller et vérifier que les systèmes que vous restaurez en production ne sont pas vulnérables aux techniques d'attaque initiales ?

Rapport post-incident

Après l'événement, AMS lance un processus d'examen des enquêtes pour tous les incidents de sécurité. AMS lance également un processus de correction d'erreur (COE) pour traiter les incidents de sécurité provoqués par un système ou une erreur procédurale susceptibles d'être améliorés. AMS s'associe à vous pour améliorer en permanence l'expérience des enquêtes de sécurité. Le processus COE aide AMS à identifier les facteurs qui contribuent aux événements ayant un impact sur le client et à relier ces causes aux mesures à prendre pour éviter que des événements similaires ne se reproduisent, ou contribuer à atténuer la durée ou le niveau de l'impact.

Le processus d'examen des enquêtes sur les incidents de sécurité aborde les points suivants afin d'identifier les opportunités d'amélioration :

- Combien de temps s'est-il écoulé entre le début de l'incident et la découverte de l'incident, jusqu'à l'évaluation initiale de l'impact et jusqu'à chaque étape du processus de gestion de l'incident (par exemple, confinement, reprise) ?
- Combien de temps a-t-il fallu à l'équipe d'intervention pour répondre au rapport initial de l'incident ?
- Combien de temps a-t-il fallu pour réaliser une première analyse d'impact ?
- Cela était-il évitable et comment ? Existe-t-il un outil ou un processus qui aurait pu empêcher cela ?
- Aurions-nous pu le détecter plus tôt et comment ?
- Qu'est-ce qui aurait pu accélérer l'enquête ?
- Les procédures documentées de réponse aux incidents ont-elles été suivies ? Étaient-ils adéquats ?
- L'échange d'informations avec les autres parties prenantes s'est-il fait en temps opportun. Comment pourrait-on l'améliorer ?
- La collaboration avec les autres équipes (AWS sécurité, équipes chargées des comptes, équipe de AWS développement et équipe de sécurité du client) a-t-elle été efficace ? Dans le cas contraire, qu'est-ce qui pourrait être amélioré ?

- Quelles sont les étapes de préparation manquantes qui auraient pu être utiles, les matrices d'escalade, les RACI, les modèles de responsabilité partagée, etc. ? Est-il nécessaire de mettre à jour un Runbook ?
- Quelle était la différence entre l'analyse d'impact initiale et l'analyse d'impact finale ? Que pouvons-nous faire pour améliorer la précision des évaluations dès le début de la réponse aux incidents ?
- Quelles sont les mesures à prendre à la lumière des leçons apprises ?

Runbooks de réponse aux incidents de sécurité dans AMS

Cette section contient deux runbooks :

- Réponse à l'activité de l'utilisateur root
- Réponse aux événements liés aux programmes malveillants

Réponse à l'activité de l'utilisateur root

L'utilisateur root est le superutilisateur de votre AWS compte. Notez qu'AMS surveille l'utilisation du root. Il est recommandé de n'utiliser l'utilisateur root que pour les quelques tâches qui le nécessitent, par exemple pour modifier les paramètres de votre compte, activer l'accès AWS Identity and Access Management (IAM) à la facturation et à la gestion des coûts, modifier votre mot de passe root et activer l'authentification multifactorielle (MFA). Pour plus d'informations, consultez la section Tâches nécessitant des informations d'identification de l'utilisateur root.

Pour plus d'informations sur la manière d'informer AMS de l'utilisation prévue du compte root, consultez Quand et comment utiliser le compte root dans AMS.

Lorsque l'activité d'un utilisateur root est détectée, il s'agit soit de tentatives infructueuses de connexion susceptibles d'indiquer une attaque par force brute, soit d'une activité sur le compte après une connexion réussie, un événement se produit et un incident est envoyé aux contacts de sécurité que vous avez définis.

AWS Managed Services Operations enquête sur les activités imprévues des utilisateurs root, collecte, triage et analyse des données, et réalise des activités de confinement selon vos instructions, suivies d'une analyse post-événement.

Si vous utilisez le modèle d'exploitation AMS Advanced, vous recevez des communications supplémentaires de la part des ingénieurs AMS CSDM et AMS Ops qui confirment l'activité imprévue de l'utilisateur root en raison de la responsabilité d'AMS de sécuriser les informations d'identification

de l'utilisateur root. AMS enquête sur l'activité de l'utilisateur root jusqu'à ce que vous confirmiez la marche à suivre.

Préparation

Informez AMS de toute utilisation prévue d'un utilisateur root en soumettant une demande de service AMS avec les données et les heures de l'événement planifié afin d'éviter toute activité de réponse inutile aux incidents.

Travaillez régulièrement GameDays avec AMS pour valider les processus de réponse aux incidents des clients d'AMS, vérifier que le personnel et les systèmes sont à jour, et renforcer la mémoire musculaire auprès des personnes responsables afin de répondre plus rapidement aux incidents.

Phase A : détecter

AMS surveille l'activité root dans les comptes par le biais de sources de détection, notamment GuardDuty la surveillance AMS.

Si vous utilisez AMS Accelerate, le modèle de fonctionnement répond à l'incident demandant une enquête en cas d'activité inattendue de l'utilisateur root. Lorsque cela se produit, AMS Operations lance le runbook du compte compromis.

Si vous utilisez AMS Advanced, le modèle opérationnel répond à l'incident ou informe le CSDM de toute activité planifiée de l'utilisateur root afin de mettre fin à une enquête en cours sur la compromission d'un compte.

Phase B : Analyse

AMS effectue une enquête approfondie sur les événements de l'utilisateur root lorsqu'il est déterminé que l'activité n'est pas autorisée. À l'aide des automatismes et de l'équipe d'intervention de sécurité AMS, les journaux et les événements sont analysés pour détecter les anomalies et les comportements inattendus des utilisateurs root. Les journaux vous sont fournis pour vous aider à déterminer si l'activité est inconnue, s'il s'agit d'un événement impliquant un utilisateur root autorisé ou s'il nécessite une enquête plus approfondie.

Voici quelques exemples des informations fournies au cours de l'enquête pour étayer les contrôles internes :

- Informations sur le compte : sur quel compte le compte root a-t-il été utilisé ?
- Adresse e-mail de l'utilisateur root : chaque utilisateur root est associé à une adresse e-mail de votre organisation

- Détails d'authentification : où et quand l'utilisateur root a-t-il accédé à votre environnement ?
- Enregistrements d'activité : qu'a fait l'utilisateur lorsqu'il s'est connecté en tant que root ? Ces enregistrements prennent la forme d' CloudWatch événements. Comprendre comment lire ces journaux facilite les recherches.

Il est recommandé que vous soyez prêt à recevoir les informations d'analyse et que vous disposiez d'un plan pour contacter les points de contact autorisés pour les comptes au sein de votre organisation. Comme les utilisateurs root ne sont pas nommés en tant qu'individus, déterminer qui a accès à l'adresse e-mail racine utilisée pour le compte au sein de votre organisation permet d'acheminer rapidement les questions en interne.

Phase C : Contenir et éradiquer

AMS travaille en partenariat avec vos équipes de sécurité pour effectuer le confinement sous la direction de vos contacts agréés chargés de la sécurité client. Les options de confinement incluent :

- Rotation des informations d'identification et des clés appropriées.
- Fin des sessions actives sur les comptes et les ressources.
- Eradiquer les ressources créées.

Au cours des activités de confinement, AMS travaille en étroite collaboration avec votre équipe de sécurité pour s'assurer que toute perturbation de vos charges de travail est minimisée et que les informations d'identification root sont correctement sécurisées.

Une fois le plan de confinement terminé, vous collaborez avec l'équipe des opérations d'AMS pour toutes les actions de restauration nécessaires.

Rapport post-incident

Selon les besoins, AMS lance le processus d'examen des enquêtes pour identifier les leçons apprises. Dans le cadre de l'élaboration d'un COE, AMS communique toutes les conclusions pertinentes aux clients concernés afin de les aider à améliorer leur processus de réponse aux incidents.

AMS documente tous les derniers détails de l'enquête, collecte les indicateurs appropriés, puis signale l'incident à toutes les équipes internes d'AMS qui ont besoin d'informations, y compris le CSDM et l'autorité de certification qui vous ont été assignés.

Réponse aux événements liés aux programmes malveillants

Les EC2 instances Amazon sont utilisées pour héberger diverses charges de travail, notamment des logiciels tiers et des logiciels développés sur mesure déployés par les équipes d'application au sein des organisations. AMS fournit et vous encourage à déployer vos charges de travail sur des images corrigées et maintenues en permanence par AMS.

Pendant le fonctionnement des instances, AMS surveille les anomalies de comportement ou d'activité par le biais de divers contrôles de détection de sécurité, notamment Amazon GuardDuty, Network Traffic et les flux internes de Threat Intelligence d'Amazon.

AMS surveille également les découvertes de GuardDuty malwares. Ils sont disponibles sur AMS Advanced et AMS Accelerate, s'ils sont activés. Consultez Malware Protection sur Amazon GuardDuty pour plus d'informations.

> **Note**
>
> Si vous avez opté pour Bring Your Own EPS, le processus de réponse aux incidents est différent de celui décrit sur cette page. Pour plus d'informations, consultez la documentation référencée.

Lorsqu'un logiciel malveillant est détecté, un incident est créé et vous en êtes informé. Cette notification est suivie de toutes les activités de correction effectuées. AMS Operations enquête, collecte, triage et analyse des données, puis réalise des activités de confinement selon vos instructions, suivies d'une analyse post-événement.

Phase A : détecter

AMS surveille les événements sur les instances avec GuardDuty. AMS détermine les activités d'enrichissement et de triage appropriées pour vous aider à prendre des décisions de confinement ou d'acceptation des risques en fonction du type de découverte ou d'alerte.

La collecte de données est effectuée en fonction du type de recherche. La collecte de données implique d'interroger plusieurs sources de données à la fois à l'intérieur et à l'extérieur du compte concerné afin de se faire une idée de l'activité observée ou des configurations préoccupantes.

AMS met en corrélation le résultat avec toute autre alarme ou alerte ou avec la télémétrie provenant des comptes concernés ou des plateformes de renseignement sur les menaces AMS.

Phase B : Analyse

Une fois les données collectées, elles sont analysées pour identifier toute activité ou tout indicateur préoccupant. Au cours de cette phase de l'enquête, AMS s'associe à vous pour intégrer les connaissances commerciales et professionnelles des instances et des charges de travail afin de comprendre ce qui est attendu et ce qui sort de l'ordinaire.

Voici quelques exemples des informations fournies au cours de l'enquête pour étayer les contrôles internes :

- Informations sur le compte : sur quel compte l'activité du logiciel malveillant a-t-elle été observée ?
- Détails de l'instance : Quelles sont les instances impliquées dans les événements malveillants ?
- Horodatage de l'événement : quand l'alerte s'est-elle déclenchée ?
- Informations sur la charge de travail : Qu'est-ce qui s'exécute sur l'instance ?
- Informations sur les malwares, le cas échéant : familles de malwares et informations Open Source sur les malwares.
- Informations sur les utilisateurs ou les rôles : quels utilisateurs ou rôles sont concernés et impliqués dans l'activité ?
- Enregistrements d'activité : Quelles activités sont enregistrées sur l'instance ? Ils prennent la forme d' CloudWatch événements et d'événements système provenant de l'instance. Comprendre comment lire ces journaux vous aidera dans vos recherches.
- Activité réseau : quels points de terminaison se connectent à l'instance, à quoi l'instance se connecte et qu'est-ce que l'analyse du trafic ?

Il est recommandé d'être prêt à recevoir des informations d'enquête et d'avoir un plan indiquant comment contacter les points de contact appropriés pour les comptes, les instances et les charges de travail au sein de votre organisation. La compréhension de la topologie de votre réseau et de la connexion attendue peut contribuer à accélérer l'analyse d'impact. La connaissance des tests d'intrusion planifiés dans l'environnement et des récents déploiements effectués par les propriétaires d'applications peut également accélérer l'investigation.

Si vous déterminez que l'activité est planifiée et autorisée, l'incident est mis à jour et l'enquête prend fin. Si la compromission est confirmée, vous déterminez avec AMS le plan de confinement approprié.

Phase C : Contenir et éradiquer

AMS travaille en partenariat avec vous pour déterminer les activités de confinement appropriées en fonction des données collectées et des informations connues. Les options de confinement incluent, sans toutefois s'y limiter :

- Préservation des données par le biais de snapshots
- Modification des règles réseau pour limiter le trafic entrant ou sortant des instances
- Modification des politiques relatives aux utilisateurs et aux rôles SCP, IAM pour limiter l'accès
- Interruption, suspension ou désactivation d'instances
- Résiliation de toute connexion persistante
- Rotation des accréditations/clés appropriés

Si vous choisissez d'exécuter une activité d'éradication sur l'instance, AMS vous aide à y parvenir. Les options incluent, sans toutefois s'y limiter :

- Suppression de tout logiciel indésirable
- Reconstruction de l'instance à partir d'une image propre entièrement corrigée et redéploiement des applications et de la configuration
- Restauration de l'instance à partir d'une sauvegarde précédente
- Déploiement d'applications et de services sur une autre instance de votre compte susceptible de convenir à l'hébergement des charges de travail.

Il est important de déterminer comment le logiciel malveillant a été diffusé et exécuté sur l'instance avant le rétablissement du service afin de s'assurer que des contrôles supplémentaires sont appliqués pour empêcher la réapparition du logiciel malveillant sur l'instance. AMS fournit des informations ou des informations supplémentaires à vos partenaires ou équipes de criminalistique si nécessaire pour soutenir la criminalistique.

À ce stade, vous travaillez avec AMS Operations pour les activités de restauration. AMS travaille en étroite collaboration avec vous afin de minimiser les perturbations des charges de travail et de sécuriser les instances.

Rapport post-incident

Au besoin, AMS lance le processus d'examen des enquêtes pour identifier les leçons apprises. Dans le cadre de l'élaboration d'un COE, AMS vous communique les résultats pertinents pour vous aider à améliorer votre processus de réponse aux incidents.

AMS documente les derniers détails de l'enquête, collecte les indicateurs appropriés et signale l'incident aux équipes internes d'AMS qui ont besoin d'informations, y compris le CSDM et le CA qui vous ont été assignés.

Enregistrement et surveillance des événements de sécurité dans Accelerate

Les comptes inscrits à AMS Accelerate sont configurés avec un déploiement de base d' CloudWatch événements et d'alarmes qui a été optimisé pour réduire le bruit et identifier les signes d'un véritable incident. AMS Accelerate l'utilise également GuardDuty pour le suivi des comptes. Pour de plus amples informations, veuillez consulter Moniteur avec GuardDuty.

Conformité des configurations dans Accelerate

AMS Accelerate vous aide à configurer vos ressources selon des normes élevées en matière de sécurité et d'intégrité opérationnelle, et à respecter les normes sectorielles suivantes :

- Centre pour la sécurité Internet (CIS)
- Cadre de sécurité cloud (CSF) du National Institute of Standards and Technology (NIST)
- Health Insurance Portability and Accountability Act (HIPAA)
- Norme de sécurité des données (DSS) de l'industrie des cartes de paiement (PCI)

Pour ce faire, nous déployons l'ensemble de nos AWS Config règles de conformité définies sur votre compte, voirBibliothèque de règles de configuration AMS. Une AWS Config règle représente les configurations souhaitées pour une ressource et est évaluée par rapport aux modifications de configuration apportées aux paramètres de vos AWS ressources. Toute modification de configuration déclenche un grand nombre de règles pour tester la conformité. Supposons, par exemple, que vous créiez un compartiment Amazon S3 et que vous le configuriez pour qu'il soit lisible par le public, en violation des normes NIST. La bucket-public-read-prohibited règle des ams-nist-cis-s 3

détecte la violation et indique que votre compartiment S3 n'est pas conforme dans votre rapport de configuration. Comme cette règle appartient à la catégorie de correction automatique des incidents, elle crée immédiatement un rapport d'incident vous alertant du problème. D'autres violations de règles plus graves peuvent amener AMS à résoudre automatiquement le problème. Consultez Réponses aux violations dans Accelerate.

> **Important**
>
> Si vous souhaitez que nous fassions davantage, par exemple, si vous souhaitez qu'AMS remédie à une violation pour vous, quelle que soit sa catégorie de correction, soumettez une demande de service demandant à AMS de corriger les ressources non conformes pour vous. Dans la demande de service, incluez un commentaire tel que « Dans le cadre de la correction des règles de configuration AMS, veuillez corriger les ressources non conformes*RESOURCE_ARNS_OR_IDs*, configurez la règle *CONFIG_RULE_NAME* dans le compte » et ajoutez les entrées requises pour remédier à la violation.
> Si vous souhaitez que nous fassions moins, par exemple, si vous ne voulez pas que nous prenions des mesures sur un compartiment S3 spécifique qui nécessite un accès public dès sa conception, vous pouvez créer des exceptions, voirCréation d'exceptions aux règles dans Accelerate.

Bibliothèque de règles de configuration AMS

Accelerate déploie une bibliothèque de règles de configuration AMS pour protéger votre compte. Ces règles de configuration commencent par `params-`. Vous pouvez consulter les règles de votre compte et leur état de conformité à partir de la AWS Config console, de la AWS CLI ou de l' AWS Config API. Pour des informations générales sur l'utilisation AWS Config, consultez la section ViewingConfiguration Conformité.

> **Note**
>
> Pour les régions cloud opt-in Régions AWS et Gov, nous ne déployons qu'un sous-ensemble des règles de configuration en raison des restrictions régionales. Vérifiez la disponibilité des règles dans les régions en vérifiant le lien associé à l'identifiant dans le tableau des règles de configuration AMS Accelerate.
> Vous ne pouvez supprimer aucune des règles de configuration AMS déployées.

Tableau des règles

Téléchargez sous le nom ams_config_rules.zip.

Règles de configuration AMS

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-guardduty-activé-centralisé	GuardDuty	Périodique	Corriger	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-1 ; HIPAA : 164.312 (a) (2) (iv), 164,312 (e) (2) (ii) ; PCI : 2.2, 3.4, 8.2.1 ;
ams-nist-cis-vpc-flow-logs-enabled	VPC	Périodique	Corriger	CIS : CIS.6 ; NIST-CSF : DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1 ; HIPAA : 164,308 (a) (3) (ii) (A), 164,312 (b) ; PCI : 2,2, 10,10,3,2, 10,3,3, 10,3,6 ;
ams-eks-secrets-encrypted	EKS	Périodique	Incident	CIS : NON ; NIST-CSF : NON ; HIPAA : NON ; PCI : NON ;
ams-eks-endpoint-no-accès public	EKS	Périodique	Incident	CIS : NON ; NIST-CSF : NON ; HIPAA : NON ; PCI : NON ;
ams-nist-cis-vpc-default-security-group-closed	VPC	Changements de configuration	Incident	CIS : CIS.11, CIS.12, CIS.9 ; NIST-CSF : DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4 ; HIPAA : 164.312 (e) (1) ; PCI : 1.2,1.3,2.1,2.1,1.3.1,1.3.2,2.2.2 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-iam-politique de mot de passe	IAM	Périodique	Incident	CIS : NA ; NIST-CSF : PR.AC-1, PR.AC-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (A), 164,308 (a) (3) (ii) (B), 164,308 (a) (4) (i), 164,308 (a) (4) (a) (4) (ii) (A) ,164308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C) ,164312 (a) (1) ; PCI : 7.1.2, 7.1.3, 7.2.1, 7.2.2 ;
ams-nist-cis-iam-root-access-key-check	IAM	Périodique	Incident	CIS : CIS.16, CIS.4 ; NIST-CSF : PR.AC-1, PR.AC-4, PR.PT-3 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (A), 164,308 (a) (3) (ii) (B), 164,308 (a) (4) (i), 164,308 (a) (a) 4) (ii) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1) ; PCI : 2.2, 7.1.2, 7.1.3, 7.2.1, 7.2.2 ;
ams-nist-cis-iam-user-mfa-enabled	IAM	Périodique	Incident	CIS : CIS.16 ; NIST-CSF : PR.AC-1, PR.AC-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (A), 164,308 (a) (3) (ii) (B), 164,308 (a) (4) (i), 164,308 (a) (4) (a) 64,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1) ; PCI : 2.2, 7.1.2, 7.1.3, 7.2.1, 7.2.2 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-restricted-ssh	Groupes de sécurité	Changements de configuration	Incident	CIS : CIS.16 ; NIST-CSF : PR.AC-1, PR.AC-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1) ; PCI : 2,2, 7,2,1, 8,1.4 ;
ams-nist-cis-restricted-ports communs	Groupes de sécurité	Changements de configuration	Incident	CEI : CIS.11, CIS.12, CIS.9 ; NIST-CSF : DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (B), 164,308 (a) (4) (i) ,164308 (a) (4) (ii)) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1), 164,312 (e) (1) ; PCI : 1,2, 1,3, 3,2, 2.2.2 ;
ams-nist-cis-s3 account-level-public-access blocs	S3	Changements de configuration	Incident	CEI : CIS.9, CIS.12, CIS.14 ; NIST-CSF : PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C), 164,312 (a) (1), 164,312 (e) (1) ; PCI : 1.2,1.2,1 .3,1.3,1.3.2,1.3.2,1.3,4, 1,3,6, 2,2, 2.2.2 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-s3- bucket-public-read-prohibited	S3	Changements de configuration	Incident	CEI : CIS.12, CIS.14, CIS.9 ; NIST-CSF : PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C), 164,312 (a) (1), 164,312 (e) (1) ; PCI : 1,2, 1,3, 2,2, 1,1.3,1, 1,3,2, 1,3,4, 1,3,4, 3,6, 2,2.2 ;
ams-nist-cis-s3- bucket-public-write-prohibited	S3	Changements de configuration	Incident	CEI : CIS.12, CIS.14, CIS.9 ; NIST-CSF : PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C), 164,312 (a) (1), 164,312 (e) (1) ; PCI : 1,2, 1,3, 2,2, 1,1.3,1, 1,3,2, 1,3,4, 1,3,4, 3,6, 2,2.2 ;
ams-nist-cis-s3 bucket-server-side-encryption - activé	S3	Changements de configuration	Incident	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-1 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (c) (2), 164,312 (e) (2) (ii) ; PCI : 2,2 3,4, 10.5, 8.2.1 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-securityhub-activé	Security Hub	Périodique	Incident	CEI : CIS.3, CIS.4, CIS.6, CIS.12, CIS.16, CIS.19 ; NIST-CSF : PR.DS-5, PR.PT-1 ; HIPAA : 164.312 (b) ; PCI : NA ;
ams-nist-cis-ec2- instance-managed-by-systems gérants	EC2	Changements de configuration	Rapport	CIS : CIS.2, CIS.5 ; NIST-CSF : ID.AM-2, PR.IP-1 ; HIPAA : 164.308 (a) (5) (ii) (B) ; PCI : 2,4 ;
ams-nist-cis-cloudtrail-activé	CloudTrail	Périodique	Rapport	CIS : CIS.16, CIS.6 ; NIST-CSF : DE.AE-1, DE.AE-3, PR.DS-5, PR.MA-2, PR.PT-1 ; HIPAA : 164,308 (a) (3) (ii) (A), 164,308 (a) (5) (ii) (C), 164,312 (b) ; PCI : 10,10,12,10,1 2, 10,2,3, 10,2,4, 10,2,5, 10,2,6, 10,2,7, 10,3,1, 10,3,2, 10,3,3, 10,3,4, 10,3,5, 10,3,6 ;
ams-nist-cis-access-touches pivotantes	IAM	Périodique	Rapport	CIS : CIS.16 ; NIST-CSF : PR.AC-1 ; HIPAA : 164,308 (a) (4) (ii) (B) ; PCI : 2,2 ;
ams-nist-cis-acm-certificate-expiration-check	Certificate Manager	Changements de configuration	Rapport	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.AC-5, PR.PT-4 ; HIPAA : NA ; PCI : 4.1 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-alb- http-to-https-redirection-vérifier	ALB	Périodique	Rapport	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-2 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (e) (1), 164,312 (e) (2) (i), 164,312 (e) (2) (ii) ; PCI : 2,3, 4.1, 8.2.1 ;
ams-nist-cis-api- gw-cache-enabled-and crypté	API Gateway	Changements de configuration	Rapport	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-1 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (e) (2) (ii) ; PCI : 3,4 ;
ams-nist-cis-api-gw-execution-logging-enabled	API Gateway	Changements de configuration	Rapport	CIS : CIS.6 ; NIST-CSF : DE.AE-1, DE.AE-3, PR.PT-1 ; HIPAA : 164.312 (b) ; PCI : 10.1, 10.3.1, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.5.4 ;
ams-nist-autoscaling-group-elb-healthcheck-required	ELB	Changements de configuration	Rapport	CIS : NA ; NIST-CSF : PR.PT-1, PR.PT-5 ; HIPAA : 164.312 (b) ; PCI : 2.2 ;
ams-nist-cis-cloud-trail-encryption-enabled	CloudTrail	Périodique	Rapport	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-1 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (e) (2) (ii) ; PCI : 2,2 3,4, 10,5 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-cloud- trail-log -file-validation activé	CloudTrail	Périodique	Rapport	CIS : CIS.6 ; NIST-CSF : PR.DS-6 ; HIPAA : 164,312 (c) (1), 164,312 (c) (2) ; PCI : 2,2, 10,5, 11,5, 10,5,2,10,5.5 ;
ams-nist-cis-cloudtrail-s3-dataevents activé	CloudTrail	Périodique	Rapport	CIS : CIS.6 ; NIST-CSF : DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1 ; HIPAA : 164,308 (a) (3) (ii) (A), 164,312 (b) ; PCI : 2,2,10,10 ,10,10.2,10.2.3,10.3.1,10.3 .130.3,10.3.4,10.3.10.3.4,1 0.3.10.3.10.3.10.3.10,3,6 ;
ams-nist-cis-cloudwatch-alarm-action-check	CloudWatch	Changements de configura tion	Rapport	CEI : CIS.13, CIS.14 ; NIST-CSF : NA ; HIPAA : 164,312 (a) (2) (iv), 164,312 (e) (2) (ii) ; PCI : 3,4 ;
ams-nist-cis-cloudwatch-log-group-en crypted	CloudWatch	Périodique	Rapport	CEI : CIS.13, CIS.14 ; NIST-CSF : NA ; HIPAA : 164,312 (a) (2) (iv), 164,312 (e) (2) (ii) ; PCI : 3,4 ;
ams-nist-cis-codebuild-project-envva r-awscred-check	CodeBuild	Changements de configura tion	Rapport	CIS : CIS.18 ; NIST-CSF : PR.DS-5 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C), 164,312 (a) (1) ; PCI : 8.2.1 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-codebuild- project-source-repo-url-vérifier	CodeBuild	Changements de configuration	Rapport	CIS : CIS.18 ; NIST-CSF : PR.DS-5 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C), 164,312 (a) (1) ; PCI : 8.2.1 ;
ams-nist-cis-db-instance-backup-enabled	RDS	Changements de configuration	Rapport	CIS : CIS.10 ; NIST-CSF : ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1 ; HIPAA : 164,308 (a) (7) (i), 164,308 (a) (7) (ii) (A), 164,308 (a) (7) (ii) (B) ; PCI : NA ;
ams-nist-cis-dms-replication-not-public	DMS	Périodique	Rapport	CEI : CIS.12, CIS.14, CIS.9 ; NIST-CSF : PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C), 164,312 (a) (1), 164,312 (e) (1) ; PCI : 1,2, 1,3, 2,1, 1,3, 1,1.3,2, 1,3,4, 1,3,4, 1,3,6, 2.2.2 ;
ams-nist-dynamodb-autoscaling-activé	DynamoDB	Périodique	Rapport	CIS : NA ; NIST-CSF : ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1 ; HIPAA : 164,308 (a) (7) (i), 164,308 (a) (7) (ii) (C) ; PCI : NA ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-dynamodbcompatible-pitr	DynamoDB	Périodique	Rapport	CIS : CIS.10 ; NIST-CSF : ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1 ; HIPAA : 164,308 (a) (7) (i), 164,308 (a) (7) (ii) (A), 164,308 (a) (7) (ii) (B) ; PCI : NA ;
ams-nist-dynamodb-throughput-contrôle des limites	DynamoDB	Périodique	Rapport	CIS : NA ; NIST-CSF : NA ; HIPAA : 164.312 (b) ; PCI : NA ;
ams-nist-ebs-optimized-instance	EBS	Changements de configuration	Rapport	CIS : NA ; NIST-CSF : NA ; HIPAA : 164.308 (a) (7) (i) ; PCI : NA ;
ams-nist-cis-ebs-snapshot-public-restorable-check	EBS	Périodique	Rapport	CEI : CIS.12, CIS.14, CIS.9 ; NIST-CSF : PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C), 164,312 (a) (1), 164,312 (e) (1) ; PCI : 1,2, 1,3, 2,1, 1,3, 1,1.3,2, 1,3,4, 1,3,4, 1,3,6, 2.2.2 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-ec2- instance-detailed-monitoring-enabled	EC2	Changements de configuration	Rapport	CIS : NA ; NIST-CSF : DE.AE-1, PR.PT-1 ; HIPAA : 164.312 (b) ; PCI : NA ;
ams-nist-cis-ec2- instance-no-public-ip	EC2	Changements de configuration	Rapport	CEI : CIS.12, CIS.14, CIS.9 ; NIST-CSF : PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C) ,164312 (a) (1), 164,312 (e) (1) ; PCI : 1,2, 1,3, 1,1.3,1, 1,3,2, 1,3,4, 1,3,4, 3,6, 2,2.2 ;
ams-nist-cis-ec2-managedinstance-association-compliance-status -vérifier	EC2	Changements de configuration	Rapport	CIS : CIS.12, CIS.9 ; NIST-CSF : PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C) ,164312 (a) (a) 1) ,164.312 (e) (1) ; PCI : 1.2,1.3,1.3,1.3,1.3.2,1.3.2 ,1.3.4, 1.3.6, 2.2.2 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-ec2-managedinstance-patch-compliance-status -vérifier	EC2	Changements de configuration	Rapport	CIS : CIS.2, CIS.5 ; NIST-CSF : ID.AM-2, PR.IP-1 ; HIPAA : 164.308 (a) (5) (ii) (B) ; PCI : 6,2 ;
ams-nist-cis-ecinstance à 2 arrêts	EC2	Périodique	Rapport	CIS : CIS.2 ; NIST-CSF : ID.AM-2, PR.IP-1 ; HIPAA : NON ; PCI : NON ;
ams-nist-cis-ec2- volume-in use-check	EC2	Changements de configuration	Rapport	CIS : CIS.2 ; NIST-CSF : PR.IP-1 ; HIPAA : NON ; PCI : NON ;
ams-nist-cis-efs-chèque crypté	EFS	Périodique	Rapport	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-1 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (e) (2) (ii) ; PCI : 3,4, 8.2.1 ;
ams-nist-cis-eip-attaché	EC2	Changements de configuration	Rapport	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-1 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (e) (2) (ii) ; PCI : 3,4, 8.2.1 ;
ams-nist-cis-elasticache-redis-cluster-automatic-backup -vérifier	ElastiCache	Périodique	Rapport	CIS : CIS.10 ; NIST-CSF : ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1 ; HIPAA : 164,308 (a) (7) (i), 164,308 (a) (7) (ii) (A), 164,308 (a) (7) (ii) (B) ; PCI : NA ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-opensearch-encrypted-at-rest	OpenSearch	Périodique	Rapport	CIS : CIS.14, CIS.13 ; NIST-CSF : PR.DS-1 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (e) (2) (ii) ; PCI : 3,4, 8.2.1 ;
ams-nist-cis-opensearch-in-vpc-only	OpenSearch	Périodique	Rapport	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-1 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (e) (2) (ii) ; PCI : 3,4, 8.2.1 ;
ams-nist-cis-elb-acm-certificate-required	Certificate Manager	Changements de configuration	Rapport	CIS : CIS.12, CIS.9 ; NIST-CSF : PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C) 64,312 (a) (1), 164,312 (e) (1) ; PCI : 1,2, 1,3, 1,1.3,1, 1,3,2, 3,4, 1,3,4, 1,3,6, 2,2.2 ;
ams-nist-elb-deletion-activé par la protection	ELB	Changements de configuration	Rapport	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-2 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (e) (1), 164,312 (e) (2) (i), 164,312 (e) (2) (ii) ; PCI : 4.1, 8.2.1 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-elb-activé pour la journalisation	ELB	Changements de configuration	Rapport	CIS : CIS.6 ; NIST-CSF : DE.AE-1, DE.AE-3, PR.PT-1 ; HIPAA : 164.312 (b) ; PCI : 10.1, 10.3.1, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.5.4 ;
ams-nist-cis-emr-compatible avec Kerberos	EMR	Périodique	Rapport	CIS : CIS.6 ; NIST-CSF : DE.AE-1, DE.AE-3, PR.PT-1 ; HIPAA : 164.312 (b) ; PCI : 10.1, 10.3.1, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6, 10.5.4 ;
ams-nist-cis-emr-master-no-public-ip	EMR	Périodique	Rapport	CIS : CIS.14, CIS.16 ; NIST-CSF : PR.AC-1, PR.AC-4, PR.AC-6 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (A), 164,308 (a) (3) (ii) (B), 164,308 (a) (4) (i), 164,308 (a) 4) (ii) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1) ; PCI : 7.2.1 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-encrypted-volumes	EBS	Changements de configuration	Rapport	CIS : CIS.12, CIS.9 ; NIST-CSF : PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C) ,164312 (a) (a) 1) ,164.312 (e) (1) ; PCI : 1.2,1.3,1.3,1.3,1.3.2,1.3.2 ,1.3.4, 1.3.6, 2.2.2 ;
ams-nist-cis-guardduty-non-archived-findings	GuardDuty	Périodique	Rapport	CEI : CIS.12, CIS.13, CIS.16, CIS.19, CIS.3, CIS.4, CIS.6, CIS.8 ; NIST-CSF : DE.AE-2, DE.AE-3, DE.CM-4, DE.DP-5, ID.RA-1, ID.RA-3, PR.DS-5, PR.PT-1 ; HIPAA : 164.308 (a) (5)) (ii) (C), 164,308 (a) (6) (ii), 164,312 (b) ; PCI : 6,1, 11,4, 5,1,2 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-iam-group-has-users-check	IAM	Changements de configuration	Rapport	CIS : NA ; NIST-CSF : PR.AC-4, PR.AC-1 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (A), 164,308 (a) (3) (ii) (B), 164,308 (a) (4) (i), 164,308 (a) (4) (a) (4) (ii) (A) ,164308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C) ,164312 (a) (1) ; PCI : 7.1.2, 7.1.3, 7.2.1, 7.2.2 ;
ams-nist-cis-iam- policy-no-statements-with -admin-access	IAM	Changements de configuration	Rapport	CIS : CIS.16 ; NIST-CSF : PR.AC-6, PR.AC-7 ; HIPAA : 164,308 (a) (4) (ii) (B), 164,308 (a) (5) (ii) (D), 164,312 (d) ; PCI : 8.2.3, 8.2.4, 8.2.5 ;
ams-nist-cis-iam-user-group-membership-check	IAM	Changements de configuration	Rapport	CIS : CIS.16, CIS.4 ; NIST-CSF : PR.AC-1, PR.AC-4, PR.PT-3 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C) ,164312 (a) (1), 164,312 (a) (2) (i) ; PCI : 2.2, 7.1.2, 7.2.1, 8.1.1 ;
ams-nist-cis-iam-user-no-policies-check	IAM	Changements de configuration	Rapport	CIS : CIS.16 ; NIST-CSF : PR.AC-1, PR.AC-7 ; HIPAA : 164,308 (a) (4) (ii) (B), 164,312 (d) ; PCI : 8,3 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-iam-user-unused-credentials-check	IAM	Périodique	Rapport	CIS : CIS.16 ; NIST-CSF : PR.AC-1, PR.AC-4, PR.PT-3 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (A), 164,308 (a) (3) (ii) (B), 164,308 (a) (4) (i), 164,308 (a) (4) ii) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1) ; PCI : 2,2, 7,1,2, 7,1,3, 7,2,1, 7,2.2 ;
ams-nist-cis-ec2- instances-in-vpc	EC2	Changements de configuration	Rapport	CEI : CIS.11, CIS.12, CIS.9 ; NIST-CSF : DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (3) (ii) (B), 164,308 (a) (4) (i) ,164308 (a) (4) (ii)) (A), 164,308 (a) (4) (ii) (B), 164,308 (a) (4) (ii) (C), 164,312 (a) (1), 164,312 (e) (1) ; PCI : 1,2, 1,3, 3,2, 2.2.2 ;
ams-nist-cis-internet-gateway-authorized-vpc-only	Internet Gateway	Périodique	Rapport	CIS : CIS.9, CIS.12 ; NIST-CSF : NON ; HIPAA : NON ; PCI : NON ;
ams-nist-cis-kms- cmk-not-scheduled-for-suppression	KMS	Périodique	Rapport	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-1 ; HIPAA : NA ; PCI : 3.5, 3.6 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-lambda-concurrency-vérifier	Lambda	Changements de configuration	Rapport	CIS : NA ; NIST-CSF : NA ; HIPAA : 164.312 (b) ; PCI : NA ;
ams-nist-lambda-dlq-vérifier	Lambda	Changements de configuration	Rapport	CIS : NA ; NIST-CSF : NA ; HIPAA : 164.312 (b) ; PCI : NA ;
ams-nist-cis-lambda-function-public-access-prohibited	Lambda	Changements de configuration	Rapport	CIS : CIS.12, CIS.9 ; NIST-CSF : PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C) 64,312 (a) (1), 164,312 (e) (1) ; PCI : 1,2, 1,3, 1,1.3,1, 1,3,2, 1,3,4, 2,2.2 ;
ams-nist-cis-lambda-intérieur-vpc	Lambda	Changements de configuration	Rapport	CIS : CIS.12, CIS.9 ; NIST-CSF : PR.AC-3, PR.AC-4, PR.AC-5, PR.PT-3, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C) ,164312 (a) (a) 1) ,164312 (e) (1) ; PCI : 1,2, 1.3, 1.3.1, 1.3.2, 1.3.2, 1.3.4, 2.2.2 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-mfa- enabled-for-iam-console-accès	IAM	Périodique	Rapport	CIS : CIS.16 ; NIST-CSF : PR.AC-7 ; HIPAA : 164.312 (d) ; PCI : 2.2, 8.3 ;
ams-nist-cis-multi-region-cloudtrail-enabled	CloudTrail	Périodique	Rapport	CIS : CIS.6 ; NIST-CSF : DE.AE-1, DE.AE-3, PR.DS-5, PR.MA-2, PR.PT-1 ; HIPAA : 164,308 (a) (3) (ii) (A), 164,312 (b) ; PCI : 2,2,10,10,10,2,10,3,10,2,4, 10,2,5, 10,2,6, 10,2,7, 10,3,1, 10,3,2, 10,3,3, 10,3,4, 10,3,5, 10,3,6 ;
ams-nist-rds-enhanced-activé pour la surveillance	RDS	Changements de configuration	Rapport	CIS : NA ; NIST-CSF : PR.PT-1 ; HIPAA : 164.312 (b) ; PCI : NA ;
ams-nist-cis-rds-instance-public-access-check	RDS	Changements de configuration	Rapport	CEI : CIS.12, CIS.14, CIS.9 ; NIST-CSF : PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C), 164,312 (a) (1), 164,312 (e) (1) ; PCI : 1,2, 1,3, 2,1, 1,3, 1,1.3,2, 1,3,4, 1,3,4, 1,3,6, 2.2.2 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-rds-multi-az-support	RDS	Changements de configuration	Rapport	CIS : NA ; NIST-CSF : ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1 ; HIPAA : 164,308 (a) (7) (i), 164,308 (a) (7) (ii) (C) ; PCI : NA ;
ams-nist-cis-rds-snapshots-public-prohibited	RDS	Changements de configuration	Rapport	CEI : CIS.12, CIS.14, CIS.9 ; NIST-CSF : PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C), 164,312 (a) (1), 164,312 (e) (1) ; PCI : 1,2, 1,3, 2,1, 1,3, 1,1.3,2, 1,3,4, 1,3,4, 1,3,6, 2.2.2 ;
ams-nist-cis-rds-stockage crypté	RDS	Changements de configuration	Rapport	CIS : CIS.13, CIS.5, CIS.6 ; NIST-CSF : DE.AE-1, DE.AE-3, PR.DS-1, PR.PT-1 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (b), 164,312 (e) (2) (ii) ; PCI : 3,4,10,10 ,10,10,10,10,10,10 ,10,10,2,10,2,10,2,3, 10,2,5, 10,3,1, 10,3,2, 10,3,3, 10,3,4, 10,3,5, 10,3,6, 8,2.1 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-redshift-cluster-configuration-check	RedShift	Changements de configuration	Rapport	CIS : CIS.6, CIS.13, CIS.5 ; NIST-CSF : DE.AE-1, DE.AE-3, PR.DS-1, PR.PT-1 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (b), 164,312 (e) (2) (ii) ; PCI : 3,4, 8,2.1, 10,2,11,2 3, 10,2,4, 10,2,5, 10,3,1, 10,3,2, 10,3,3, 10,3,4, 10,3,5, 10,3,6 ;
ams-nist-cis-redshift-cluster-public-access-check	RedShift	Changements de configuration	Rapport	CEI : CIS.12, CIS.14, CIS.9 ; NIST-CSF : PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C), 164,312 (a) (1), 164,312 (e) (1) ; PCI : 1,2, 1,3, 2,1, 1,3, 1,1.3,2, 1,3,4, 1,3,4, 1,3,6, 2.2.2 ;
ams-nist-cis-redshift-require-tls-ssl	RedShift	Périodique	Rapport	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-2 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (e) (1), 164,312 (e) (2) (i), 164,312 (e) (2) (ii) ; PCI : 2.3, 4.1 ;
ams-nist-cis-root-account-hardware-mfa-enabled	IAM	Périodique	Rapport	CIS : CIS.16, CIS.4 ; NIST-CSF : PR.AC-7 ; HIPAA : 164.312 (d) ; PCI : 2.2, 8.3 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-root-account-mfa-enabled	IAM	Périodique	Rapport	CIS : CIS.16, CIS.4 ; NIST-CSF : PR.AC-7 ; HIPAA : 164.312 (d) ; PCI : 2.2, 8.3 ;
ams-nist-cis-s3- bucket-default-lock-enabled	S3	Changements de configuration	Rapport	CEI : CIS.14, CIS.13 ; NIST-CSF : ID.BE-5, PR.PT-5, RC.RP-1 ; HIPAA : NON ; PCI : NON ;
ams-nist-cis-s3- bucket-logging-enabled	S3	Changements de configuration	Rapport	CIS : CIS.6 ; NIST-CSF : DE.AE-1, DE.AE-3, PR.DS-5, PR.PT-1 ; HIPAA : 164,308 (a) (3) (ii) (A), 164.312 (b) ; PCI : 2.2,10,10.2,10.2,10.2.3,10.2,3,10.2.7,10.3.1,13.2,10.2,10.3, 10,3,4, 10,3,5, 10,3,6 ;
ams-nist-cis-s3- bucket-replication-enabled	S3	Changements de configuration	Rapport	CIS : CIS.10 ; NIST-CSF : ID.BE-5, PR.DS-4, PR.IP-4, PR.PT-5, RC.RP-1 ; HIPAA : 164,308 (a) (7) (i), 164,308 (a) (7) (ii) (A), 164,308 (a) (7) (ii) (B) ; PCI : 2,2, 10,5,3 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-s3- bucket-ssl-requests-only	S3	Changements de configuration	Rapport	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-2 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (c) (2), 164,312 (e) (1), 164,312 (e) (2) (i), 164,312 (e) (2) (ii) ; PCI : 2.2, 4.1, 8.2.1 ;
ams-nist-cis-s3- bucket-versioning-enabled	S3	Périodique	Rapport	CIS : CIS.10 ; NIST-CSF : ID.BE-5, PR.DS-4, PR.DS-6, PR.IP-4, PR.PT-5, RC.RP-1 ; HIPAA : 164,308 (a) (7) (i), 164,308 (a), 164,308 (a) (7) (ii) (B) ,164312 (a) c) (1), 164,312 (c) (2) ; PCI : 10.5.3 ;
ams-nist-cis-sagemaker-endpoint-configuration-kms-key - configuré	SageMaker	Périodique	Rapport	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-1 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (e) (2) (ii) ; PCI : 3,4, 8.2.1 ;
ams-nist-cis-sagemaker-notebook-instance-kms-key -configuré	SageMaker	Périodique	Rapport	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-1 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (e) (2) (ii) ; PCI : 3,4, 8.2.1 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-sagemaker-notebook-no-direct-internet-accès	SageMaker	Périodique	Rapport	CIS : CIS.12, CIS.9 ; NIST-CSF : PR.AC-3, PR.AC-4, PR.AC-5, PR.DS-5, PR.PT-3, PR.PT-4 ; HIPAA : 164,308 (a) (3) (i), 164,308 (a) (4) (ii) (A), 164,308 (a) (4) (ii) (C) 64,312 (a) (1), 164,312 (e) (1) ; PCI : 1,2, 1,3, 1,1.3,1, 1,3,2, 3,4, 1,3,4, 1,3,6, 2,2.2 ;
ams-nist-cis-secretsmanager-rotation-enabled-check	Secrets Manager	Changements de configuration	Rapport	CIS : CIS.16 ; NIST-CSF : PR.AC-1 ; HIPAA : 164.308 (a) (4) (ii) (B) ; PCI : NA ;
ams-nist-cis-secretsmanager-scheduled-rotation-success-check	Secrets Manager	Changements de configuration	Rapport	CIS : CIS.16 ; NIST-CSF : PR.AC-1 ; HIPAA : 164.308 (a) (4) (ii) (B) ; PCI : NA ;
ams-nist-cis-sns-kms chiffrés	SNS	Changements de configuration	Rapport	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-1 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (e) (2) (ii) ; PCI : 8.2.1 ;

Nom de règle	Service	Déclencheur	Action	Frameworks
ams-nist-cis-vpc- sg-open-only-to -ports autorisés	VPC	Changements de configuration	Rapport	CIS : CIS.11, CIS.12, CIS.9 ; NIST-CSF : DE.AE-1, PR.AC-3, PR.AC-5, PR.PT-4 ; HIPAA : 164.312 (e) (1) ; PCI : 1.2,1.3,1.2.1,1.3.2,1.3.2,2.2.2 ;
ams-nist-vpc-vpn-2 tunnels vers le haut	VPC	Changements de configuration	Rapport	CIS : NA ; NIST-CSF : ID.BE-5, PR.DS-4, PR.PT-5, RC.RP-1 ; HIPAA : 164.308 (a) (7) (i) ; PCI : NA ;
ams-cis-ec2-ebs-encryption-by-default	EC2	Périodique	Rapport	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-1 ; HIPAA : 164.312 (a) (2) (iv), 164,312 (e) (2) (ii) ; PCI : 2.2, 3.4, 8.2.1 ;
ams-cis-rds-snapshot-crypté	RDS	Changements de configuration	Rapport	CIS : CIS.13, CIS.14 ; NIST-CSF : PR.DS-1 ; HIPAA : 164,312 (a) (2) (iv), 164,312 (e) (2) (ii) ; PCI : 3,4, 8.2.1 ;
ams-cis-redshift-cluster-paramètres de maintenance - vérification	RedShift	Changements de configuration	Rapport	CIS : CIS.5 ; NIST-CSF : PR.DS-4, PR.IP-1, PR.IP-4 ; HIPAA : 164,308 (a) (5) (ii) (A), 164,308 (a) (7) (ii) (A) ; PCI : 6,2 ;

Réponses aux violations dans Accelerate

Toutes les violations des règles de configuration apparaissent dans votre rapport de configuration. Il s'agit d'une réponse universelle. En fonction de la catégorie de correction (gravité) de la règle, AMS peut prendre des mesures supplémentaires, résumées dans le tableau suivant. Pour plus d'informations sur la personnalisation du code d'action pour certaines règles, consultezConstatations et réponses personnalisées.

Mesures correctives

Code d'action	Actions de l'AMS
Rapport	1. Ajouter au rapport de configuration
Incident	1. Ajouter au rapport de configuration 2. Rapport d'incident automatique dans Accelerate
Corriger	1. Ajouter au rapport de configuration 2. Rapport d'incident automatique dans Accelerate 3. Correction automatique dans Accelerate

Demande d'aide supplémentaire

> **Note**
>
> AMS peut remédier à toute violation pour vous, quelle que soit sa catégorie de correction. Pour demander de l'aide, soumettez une demande de service et indiquez les ressources que vous souhaitez qu'AMS corrige avec un commentaire tel que « Dans le cadre de la correction des règles de configuration AMS, veuillez corriger la *RESOURCE_ARNS_OR_IDs* ressource de ressources non conformes ARNs/IDs>, règle de configuration *CONFIG_RULE_NAME* dans le compte » et ajoutez les entrées requises pour remédier à la violation.

AMS Accelerate dispose d'une bibliothèque de documents AWS Systems Manager d'automatisation et de runbooks pour aider à remédier aux ressources non conformes.

Ajouter au rapport de configuration

AMS génère un rapport de configuration qui suit l'état de conformité de toutes les règles et ressources de votre compte. Vous pouvez demander le rapport à votre CSDM. Vous pouvez également vérifier l'état de conformité à partir de la console AWS Config, de la AWS CLI ou de l'API AWS Config. Votre rapport de configuration inclut :

- Les principales ressources non conformes de votre environnement, pour découvrir les menaces potentielles et les erreurs de configuration
- Conformité des ressources et des règles de configuration au fil du temps
- Config : descriptions des règles, sévérité des règles et mesures correctives recommandées pour corriger les ressources non conformes

Lorsqu'une ressource passe dans un état non conforme, le statut de la ressource (et le statut de la règle) devient Non conforme dans votre rapport de configuration. Si la règle appartient à la catégorie de correction Config Report Only, AMS n'entreprend aucune autre action par défaut. Vous pouvez toujours créer une demande de service pour demander une aide supplémentaire ou des mesures correctives à AMS.

Pour plus de détails, consultez AWS Config Reporting.

Rapport d'incident automatique dans Accelerate

En cas de violation des règles modérément grave, AMS crée automatiquement un rapport d'incident pour vous informer qu'une ressource est devenue non conforme et vous demande quelles actions vous souhaitez effectuer. Les options suivantes s'offrent à vous lorsque vous répondez à un incident :

- Demandez à AMS de corriger les ressources non conformes répertoriées dans l'incident. Ensuite, nous tentons de remédier à la ressource non conforme et nous vous informons une fois que l'incident sous-jacent a été résolu.
- Vous pouvez résoudre l'élément non conforme manuellement dans la console ou via votre système de déploiement automatique (par exemple, les mises à jour du modèle de CI/CD pipeline) ; vous pouvez ensuite résoudre l'incident. La ressource non conforme est réévaluée conformément au calendrier de la règle et, si la ressource est jugée non conforme, un nouveau rapport d'incident est créé.
- Vous pouvez choisir de ne pas résoudre la ressource non conforme et de simplement résoudre l'incident. Si vous mettez à jour la configuration de la ressource ultérieurement, AWS Config

déclenchera une réévaluation et vous serez à nouveau alerté pour évaluer la non-conformité de cette ressource.

Correction automatique dans Accelerate

Les règles les plus critiques appartiennent à la catégorie Auto Remediate. Le non-respect de ces règles peut avoir un impact important sur la sécurité et la disponibilité de vos comptes. Lorsqu'une ressource enfreint l'une de ces règles :

1. AMS vous avertit automatiquement par un rapport d'incident.
2. AMS lance une correction automatique à l'aide de nos documents SSM automatisés.
3. AMS met à jour le rapport d'incident en cas de réussite ou d'échec de la correction automatique.
4. En cas d'échec de la correction automatique, un ingénieur AMS enquête sur le problème.

Création d'exceptions aux règles dans Accelerate

La fonctionnalité d'exception de AWS Config Rules ressource vous permet de supprimer le signalement de ressources spécifiques non conformes à des règles spécifiques.

> **Note**
>
> Les ressources exemptées apparaissent toujours comme non conformes dans votre console AWS Config Service. Les ressources exemptées apparaissent avec un indicateur spécial dans Config Reports (Resource_Exception:True). CSDMs Vous pouvez filtrer ces ressources en fonction de cette colonne lorsque vous générez des rapports.

Si vous savez que certaines de vos ressources ne sont pas conformes, vous pouvez supprimer une ressource spécifique pour une règle de configuration spécifique dans leurs rapports de configuration. Pour cela :

Soumettez une demande de service à Accelerate pour votre compte, avec une liste des règles de configuration et des ressources à exempter du rapport. Vous devez fournir une justification commerciale explicite (par exemple, vous n'avez pas besoin de le signaler *`resource_name_1`* et vous n'*`resource_name_2`*êtes pas sauvegardé car nous ne voulons pas qu'ils soient sauvegardés). Pour obtenir de l'aide pour soumettre une demande de service Accelerate, consultezCréation d'une demande de service dans Accelerate.

Collez dans la demande les entrées suivantes (pour chaque ressource, ajoutez un bloc séparé avec tous les champs obligatoires, comme indiqué), puis soumettez :

```
[
    {
        "resource_name": "resource_name_1",
        "config_rule_name": "config_rule_name_1",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    },
    {
        "resource_name": "resource_name_2",
        "config_rule_name": "config_rule_name_2",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    }
]
```

Réduisez AWS Config les coûts dans Accelerate

Vous pouvez réduire les coûts d'AWS Config en utilisant l'option permettant d'enregistrer régulièrement le type de `AWS::EC2::Instance` ressource. L'enregistrement périodique enregistre les derniers changements de configuration de vos ressources une fois toutes les 24 heures, réduisant ainsi le nombre de modifications apportées. Lorsque cette option est activée, elle enregistre AWS Config uniquement la dernière configuration d'une ressource à la fin d'une période de 24 heures. Cela vous permet d'adapter les données de configuration à des cas d'utilisation spécifiques en matière de planification opérationnelle, de conformité et d'audit qui ne nécessitent pas de surveillance continue. Cette modification n'est recommandée que si vos applications dépendent d'architectures éphémères, ce qui signifie que vous augmentez ou diminuez constamment le nombre d'instances.

Pour activer l'enregistrement périodique pour le type de `AWS::EC2::Instance` ressource, contactez votre équipe de livraison AMS.

Constatations et réponses personnalisées

Vous pouvez choisir la manière dont vous souhaitez qu'AMS Accelerate réponde à certaines constatations (règles de configuration non conformes). Vous pouvez configurer AMS pour qu'il réponde aux constatations en corrigeant la constatation, en demandant votre approbation pour y remédier ou simplement en vous faisant rapport dans votre prochaine revue commerciale mensuelle (MBR). Vous pouvez modifier les réponses par défaut pour les règles AMS Accelerate Config. Pour

consulter les règles, accédez à Configuration Conformité > Tableau des règles ou téléchargez le tableau des règles sous forme de fichier ZIP ams_config_rules.zip.

La modification des réponses par défaut vous permet d'améliorer l'état de sécurité et de conformité de votre compte en permettant de corriger davantage de résultats. Lorsque vous corrigez un plus grand nombre de résultats, vous avez moins de cas à attendre pour une révision et une approbation manuelles. La vaste bibliothèque de runbooks de remédiation AMS corrige en permanence les ressources non conformes et vous n'êtes contacté que lorsque cela est nécessaire.

Les réponses personnalisées ne sont utilisées qu'avec de nouvelles ressources ou avec des ressources existantes présentant de nouveaux événements. Par exemple, une ressource devenue non conforme à la suite d'une modification. Cela s'explique par le fait que les anciennes ressources ont tendance à nécessiter une inspection plus approfondie avant d'être corrigées et qu'il est plus facile d'appliquer la correction des ressources au fur et à mesure de leur création ou de leur modification. Pour demander la correction de la recherche pour une ressource à tout moment, soumettez une demande de service.

Demande de modification des réponses par défaut

Les architectes du cloud (CAs) travaillent avec vous lors de l'intégration pour recueillir vos préférences. CAspuis configurez la configuration initiale sur les systèmes AMS internes. Après l'intégration, créez une demande de service pour demander des mises à jour de vos configurations. Vous pouvez demander des mises à jour de configuration autant de fois que nécessaire. Veuillez noter que Operations met uniquement à jour les configurations pour le compte dans lequel la demande de service a été créée. Si vous devez mettre à jour plusieurs comptes en même temps, contactez votre architecte cloud. Votre autorité de certification vous demandera de supprimer une demande de service en fonction de vos préférences à des fins d'audit.

Modification des réponses par défaut pour vos résultats et vos comptes

Vous avez toujours besoin d'une préférence de réponse pour chaque compte et chaque résultat. AMS fournit une réponse par défaut (voir Conformité des configurations), cette configuration est donc facultative. Vous pouvez remplacer les réponses par défaut pour chaque résultat par les options suivantes :

- Corriger : AMS corrige le résultat manuellement ou automatiquement. AMS examine la correction et vous avertit en cas d'échec.

- Demande d'approbation : AMS crée un dossier sortant pour vous informer de la découverte. Utilisez cette option lorsque vous souhaitez examiner le résultat avant d'approuver sa correction ou de l'exempter. AMS exécute ensuite l'action que vous préférez.
- Aucune action (rapport uniquement) : AMS ne prend aucune mesure pour corriger ou aggraver le résultat. Les résultats peuvent toujours apparaître sur la console et les rapports présentés pendant MBRs.

> **Note**
>
> Vous ne pouvez pas modifier la configuration des règles qui doivent être corrigées par AMS. Par exemple, activer Amazon GuardDuty et VPC Flow Logs.

Modification des réponses par défaut par ressource

Vous pouvez également configurer la réponse à des ressources spécifiques à l'aide de balises. Vous pouvez utiliser vos balises ou ressources de balises préexistantes à l'aide de Resource Tagger. Pour plus de détails, voirAccélérez Resource Tagger). La configuration des ressources avec des balises a priorité sur l'action par défaut pour la recherche. Lorsqu'une ressource possède plusieurs balises associées à différentes configurations, AMS ne peut pas exécuter de corrections personnalisées. AMS vous envoie plutôt une demande de service sortante pour vous informer de la situation. Par exemple, pour la recherche bucket-server-side-encryptionactivée par s3, vous pouvez :

- Modifiez la réponse pour « corriger » les compartiments S3 non chiffrés avec la paire clé-valeur de balise « Regulated : True »
- Remplacez la réponse par « aucune action » lorsque les compartiments S3 non chiffrés comportent les balises « Regulated : False », et
- Remplacez la réponse par défaut des compartiments S3 non chiffrés par « demander l'approbation ». Cela s'applique à tous les compartiments S3 qui ne possèdent pas les balises « Regulated : True » ou « Regulated : False »

Vous pouvez également ajouter l'entrée requise pour exécuter une réponse de recherche personnalisée. Par exemple, pour les corrections qui nécessitent une clé de chiffrement, vous pouvez fournir votre clé IDs à AMS. Vous pouvez modifier les paramètres d'entrée des runbooks de correction, mais AMS ne prend pas en charge l'intégration avec les runbooks personnalisés. Pour

une description des runbooks de correction AMS dans le rapport de configuration, consultez. AWS Config Rapport de conformité des contrôles

Réponse aux incidents dans Accelerate

Dès réception d'une alerte, l'équipe AMS utilise des mesures correctives automatisées et manuelles pour remettre les ressources en bon état. Si les mesures correctives échouent, AMS lance le processus de gestion des incidents afin de collaborer avec votre équipe. Vous pouvez modifier les lignes de base en mettant à jour la configuration par défaut dans un fichier de configuration.

Réponse aux incidents et intégration dans AMS Accelerate

Lors de l'intégration, AMS Accelerate supprime la création automatique d'incidents pour vos ressources non conformes existantes ; au lieu de cela, votre Cloud Service Deliver Manager (CSDM) vous fournit un rapport contenant toutes les règles de non-conformité et les ressources à examiner. Après avoir identifié les règles auxquelles vous souhaitez qu'AMS corrige, créez une demande de service dans la console Support Center indiquant ces règles et ces ressources. Le modèle de demande de service suivant est un exemple de demande d'un client adressée à AMS pour corriger manuellement les ressources non conformes. Si AMS a d'autres questions, nous collaborons avec vous dans le cadre de la demande de service afin de recueillir les informations requises.

```
Hello,
Please remediate the following resources for the Config Rule "ENCRYPTED_VOLUMES".
Resource List:
    "Vol-12345678"
    "Vol-87654312"
Thank you
```

Une fois le processus d'intégration terminé, AMS Accelerate crée automatiquement un incident pour chaque ressource non conforme aux règles marquées comme Incident automatique.

Résilience dans Accelerate

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Les zones de disponibilité vous permettent de concevoir et d'exploiter des applications et des bases de données qui basculent automatiquement entre les zones sans interruption. Les zones de disponibilité sont plus hautement

disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles de centres de données uniques ou multiples.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Pour plus d'informations sur la gestion de la continuité AMS Accelerate, consultezGestion de la continuité dans AMS Accelerate.

Contrôle de sécurité pour les systèmes end-of-support d'exploitation

Les systèmes d'exploitation qui sont en dehors de la période de support général du fabricant du système d'exploitation « end-of-support » ou d'EOS, et qui ne reçoivent pas de mises à jour de sécurité, présentent un risque de sécurité accru.

AWS propose certains services pour aider à gérer le système d'exploitation end-of-support. Pour plus d'informations sur Windows end-of-support, consultez End-of-Supportla section Programme de migration pour Windows Server.

> **Note**
>
> Des informations supplémentaires sur ce sujet sont disponibles en accédant aux rapports AWS Artifact. Pour de plus amples informations, veuillez consulter Téléchargement des rapports dans AWS Artifact. Pour accéder à AWS Artifact, vous pouvez contacter votre CSDM pour obtenir des instructions ou consulter Getting Started with AWS Artifact. Ces informations ne sont pas incluses dans ce guide de l'utilisateur car il contient des informations de sécurité sensibles.

Bonnes pratiques en matière de sécurité dans Accelerate

AMS Accelerate utilise des packs de conformité, qui fournissent un cadre de conformité à usage général conçu pour vous permettre de créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts à l'aide d'actions gérées ou personnalisées AWS Config Rules et d'actions correctives. AWS Config Pour plus d'informations sur la meilleure façon de configurer ces packs de conformité, consultez AWS Config les meilleures pratiques opérationnelles pour le NIST CSF et les meilleures pratiques opérationnelles pour les 20 meilleures pratiques du CIS.

Examens de sécurité des demandes de modification

Le processus d'examen des demandes de modification d'AWS Managed Services garantit qu'AMS effectue un examen de sécurité des modifications demandées au fur et à mesure qu'elles sont mises en œuvre en votre nom sur votre compte.

Normes techniques AMS Acceleratedéfinissez les critères de sécurité, les configurations et les processus minimaux pour établir la sécurité de base de vos comptes. Lorsque AMS met en œuvre les modifications demandées, nous respectons ces normes.

AMS évalue toutes les demandes de modification par rapport aux normes techniques AMS. Toute modification susceptible de réduire le niveau de sécurité de votre compte en s'écartant des normes techniques est soumise à un processus de vérification de sécurité. Au cours de ce processus, les risques pertinents sont mis en évidence par AMS, puis examinés et approuvés par votre approbateur de risques agréé afin de trouver un équilibre entre la sécurité et les besoins commerciaux.

Processus de gestion des risques liés à la sécurité des clients

Le processus AMS Accelerate Customer Security Risk Management (CSRM) permet d'identifier clairement les risques et de les communiquer aux propriétaires concernés. Ce processus minimise les risques de sécurité dans votre environnement et réduit les frais opérationnels permanents liés aux risques identifiés.

Par défaut, lorsqu'un membre de votre organisation demande à AMS de mettre en œuvre une modification de votre environnement géré, AMS examine la modification afin de déterminer si la demande ne respecte pas les normes techniques, ce qui est susceptible de modifier le niveau de sécurité de votre compte. En cas de risque de sécurité élevé ou très élevé, la révision des modifications est acceptée ou rejetée par votre personnel de sécurité autorisé. Les modifications demandées sont également évaluées pour détecter les effets négatifs sur la capacité d'AMS à gérer le compte. Si l'examen révèle d'éventuels effets négatifs, des examens et des approbations supplémentaires sont requis au sein de l'AMS.

Vous pouvez vous désinscrire du flux de travail basé sur l'approbation dans le processus CSRM en cas de risques élevés ou très élevés. Pour modifier l'option CSRM pour des comptes spécifiques, de la CSRM standard à la fonctionnalité de notification uniquement, collaborez avec vos responsables de prestation de services cloud pour créer une acceptation des risques unique. Si vous choisissez d'utiliser l'option Notification uniquement, AMS implémente les modifications demandées quelle que soit la catégorie de risque. De plus, AMS envoie une notification de risque à vos approbateurs de risques autorisés au lieu de demander une approbation avant la mise en œuvre du changement.

Adressez-vous à vos architectes cloud ou à vos responsables de prestation de services cloud pour plus d'informations sur le processus de CSRM d'AMS, sur la modification de l'option CSRM par défaut lors de l'intégration de nouveaux comptes AMS ou sur la mise à jour de comptes existants.

> **Note**
>
> AMS vous recommande vivement d'utiliser l'option CSRM standard par défaut dans tous vos comptes.

Normes techniques AMS Accelerate

Les catégories de normes techniques Accelerate sont les suivantes :

ID	Catégorie
AMS-STD-X002	AWS Identity and Access Management
AMS-STD-X003	Sécurité du réseau
AMS-STD-X004	Tests de pénétration
AMS-STD-X005	Amazon GuardDuty
AMS-STD-X007	Journalisation

Commandes standard dans AMS Accelerate

Les commandes standard d'AMS sont les suivantes :

AMS-STD-X002 - (IAM) AWS Identity and Access Management

ID	Norme technique
1.0	Durée du délai d'attente
1.1	Le délai d'expiration par défaut d'une session d'utilisateur fédéré est d'une heure et peut être porté à quatre heures.

ID	Norme technique
1.2	Le délai d'expiration de session RDP pour Microsoft Windows Server est fixé à 15 minutes et peut être prolongé en fonction du cas d'utilisation.
2.0	AWS Utilisation du compte root
2.1	Si un compte root est utilisé pour une quelconque raison, Amazon GuardDuty doit être configuré pour générer des résultats pertinents.
2.2	Les clés d'accès pour le compte root ne doivent pas être créées.
3,0	Création et modification d'utilisateurs
3.1	Un IAM users/roles doté d'un accès programmatique et d'autorisations en lecture seule peut être créé sans aucune politique limitée dans le temps. Toutefois, l'autorisation d'autoriser la lecture d'objets (par exemple, S3 :GetObject) dans tous les compartiments Amazon Simple Storage Service du compte n'est pas autorisée.
3.1.1	Les utilisateurs humains IAM autorisés à accéder à la console et dotés d'autorisations en lecture seule peuvent être créés avec la politique limitée dans le temps (jusqu'à 180 jours), tandis que removal/renewal/extension la politique limitée dans le temps entraînera la notification des risques. Toutefois, l'autorisation d'autoriser la lecture d'objets (par exemple, S3 :GetObject) dans tous les compartiments S3 du compte n'est pas autorisée.

ID	Norme technique
3.2	Les utilisateurs et les rôles IAM pour l'accès à la console et à la programmation avec des autorisations susceptibles de modifier l'infrast ructure (écriture et gestion des autorisations) dans le compte client ne doivent pas être créés sans acceptation des risques. Des exception s existent pour les autorisations d'écriture au niveau de l'objet S3, qui sont autorisées sans risque d'acceptation du risque, à condition que les compartiments spécifiques entrent dans le champ d'application et que les opérations de balisage soient effectuées sur des balises non liées à AMS.
3.3	Sur les serveurs Microsoft Windows, seul le compte de service géré de groupe Microsoft (GMSA) doit être créé.
4,0	Politiques, actions et APIs
4,4	Une politique ne doit pas fournir un accès administrateur avec une déclaration équivalen te à « Effet » : « Autoriser » avec « Action » : « * » au-dessus de « Ressource » : « * » sans acceptation du risque.
4.6	Les appels d'API à l'encontre des politiques clés KMS relatives aux clés d'infrastructure AMS figurant dans les politiques IAM du client ne doivent pas être autorisés.
4.8	Les actions qui modifient les enregistrements DNS de l'infrastructure AMS dans Amazon Route 53 ne doivent pas être autorisées.

ID	Norme technique
4,9	Les utilisateurs humains IAM dotés d'un accès à la console créé après avoir suivi une procédure régulière ne doivent pas être directement attachés à des politiques, à l'exception de la politique de confiance, de l'acceptation du rôle et de la politique limitée dans le temps.
4,10	Il est possible de créer des profils d' EC2 instance Amazon dotés d'un accès en lecture à un secret ou à un espace de noms spécifiqu e AWS Secrets Manager au sein du même compte.
4,12	La politique IAM ne doit inclure aucune action incluant l'action Autoriser les journaux : DeleteLogGroup et les journaux : DeleteLog Stream sur un groupe de CloudWatch journaux AMS Amazon.
4,13	Les autorisations permettant de créer des clés multirégionales ne doivent pas être autorisées.
4,14	L'accès à l'ARN du compartiment S3 qui n'est pas encore créé dans les comptes clients peut être fourni en restreignant l'accès aux compartiments aux comptes clients en spécifiant le numéro de compte à l'aide de la clé de condition S3 spécifique au service s3 :. ResourceAccount
4.15.1	Vous pouvez consulter, créer, répertorier et supprimer l'accès à votre tableau de bord personnalisé S3 Storage Lens.

ID	Norme technique
4,16	Les autorisations complètes associées à SQL Workbench peuvent être accordées pour travailler sur roles/users les bases de données Amazon Redshift.
4,17	Toutes AWS CloudShell les autorisations peuvent être accordées aux rôles des clients comme alternative à la CLI.
4,18	Un rôle IAM avec le AWS service comme principal de confiance doit également être conforme aux normes techniques IAM.
4,19	Les rôles liés au service (SLRs) ne sont pas soumis aux normes techniques d'AMS IAM, car ils sont créés et maintenus par l'équipe de service IAM.
4,20	La politique IAM ne doit pas autoriser la lecture d'objets (par exemple, S3 :GetObject) dans tous les compartiments S3 du compte.
4,21	Toutes les autorisations IAM pour le type de ressource « savingsplan » peuvent être accordées aux clients.
4,22	L'ingénieur AMS n'est pas autorisé à copier ou à déplacer les données clients (fichiers, objets S3, bases de données, etc.) manuellement dans les services de stockage de données tels qu'Amazon S3, Amazon Relational Database Service, Amazon DynamoDB, etc., ou dans le système de fichiers du système d'exploitation.
6.0	Politiques relatives aux comptes multiples

ID	Norme technique
6.1	Les politiques de confiance relatives aux rôles IAM entre les comptes AMS appartenant au même client, selon les dossiers des clients, peuvent être configurées.
6.2	Les politiques de confiance relatives aux rôles IAM entre les comptes AMS et non-AMS doivent être configurées uniquement si le compte non-AMS appartient au même client AMS (en confirmant qu'ils appartiennent au même AWS Organizations compte ou en faisant correspondre le domaine de messagerie au nom de l'entreprise du client).
6.3	Les politiques de confiance relatives aux rôles IAM entre les comptes AMS et les comptes tiers ne doivent pas être configurées sans acceptation des risques.
6.4	Des politiques inter-comptes permettant d'accéder à n'importe quel client géré CMKs entre les comptes AMS d'un même client peuvent être configurées.
6,5	Des politiques inter-comptes permettant à un compte AMS d'accéder à n'importe quelle clé KMS d'un compte non-AMS peuvent être configurées.
6,6	Les politiques inter-comptes permettant à un compte tiers d'accéder à toute clé KMS d'un compte AMS ne doivent pas être autorisées sans acceptation des risques.

ID	Norme technique
6.6.1	Les politiques inter-comptes permettant d'accéder à n'importe quelle clé KMS d'un compte AMS par un compte non-AMS ne peuvent être configurées que si le compte non-AMS appartient au même client AMS.
6.7	Des politiques inter-comptes permettant d'accéder à toutes les données ou ressources du compartiment S3 où les données peuvent être stockées (comme Amazon RDS, Amazon DynamoDB ou Amazon Redshift) entre les comptes AMS d'un même client peuvent être configurées.
6.8	Des politiques inter-comptes permettant d'accéder à toutes les données ou ressources du compartiment S3 où les données peuvent être stockées (comme Amazon RDS, Amazon DynamoDB ou Amazon Redshift) dans un compte autre qu'AMS à partir d'un compte AMS avec accès en lecture seule peuvent être configurées.

ID	Norme technique
6.9	Les politiques inter-comptes permettant d'accéder aux données du compartiment S3 ou aux ressources où les données peuvent être stockées (comme Amazon RDS, Amazon DynamoDB ou Amazon Redshift) avec des autorisations d'écriture depuis AMS vers un compte non-AMS (ou un compte non-AMS vers AMS) doivent être configurées uniquement si le compte non-AMS appartient au même client AMS (en confirmant qu'il est sous le même compte ou en faisant correspondre le domaine de messagerie avec AWS Organizations le nom de l'entreprise du client).
6,10	Des politiques inter-comptes permettant d'accéder à toutes les données ou ressource s du compartiment S3 où les données peuvent être stockées (comme Amazon RDS, Amazon DynamoDB ou Amazon Redshift) dans un compte tiers à partir d'un compte AMS avec accès en lecture seule peuvent être configuré es.
6,11	Les politiques inter-comptes permettant d'accéder aux données du compartiment S3 ou aux ressources où les données peuvent être stockées (comme Amazon RDS, Amazon DynamoDB ou Amazon Redshift) dans un compte tiers à partir d'un compte AMS avec accès en écriture ne doivent pas être configuré es.

ID	Norme technique
6,12	Les politiques entre comptes provenant de comptes tiers permettant d'accéder au compartiment S3 d'un client AMS ou à des ressources où les données peuvent être stockées (comme Amazon RDS, Amazon DynamoDB ou Amazon Redshift) ne doivent pas être configurées sans acceptation du risque.
7,0	Groupes d'utilisateurs
7.1	Les groupes IAM dotés d'autorisations en lecture seule et non mutatives sont autorisés.
8,0	Stratégies basées sur les ressources
8,4	Les ressources de l'infrastructure AMS doivent être protégées contre toute gestion par des identités non autorisées en y attachant des politiques basées sur les ressources.
8.2	Les ressources du client doivent être configuré es selon des politiques basées sur le moindre privilège, sauf si le client spécifie explicitement une politique différente.

AMS-STD-X003 - Sécurité réseau

Voici le contrôle standard pour X003 - Network Security :

ID	Norme technique
	Réseaux
1.0	Réservé pour un futur contrôle

ID	Norme technique
2.0	L'adresse IP élastique sur EC2 les instances est autorisée
3.0	Le plan de contrôle AMS et par extension le plan de données TLS 1.2+ doivent être utilisés.
5.0	Un groupe de sécurité ne doit pas avoir comme source 0.0.0.0/0 dans la règle entrante s'il n'est pas attaché à un équilibreur de charge conformément à la version 9.0
6.0	Le bucket ou les objets S3 ne doivent pas être rendus publics sans acceptation des risques.
7.0	L'accès à la gestion des serveurs sur les ports SSH/22 ou SSH/2222 (pas SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/CITRIX/1494 ou 1604, LDAP/389 ou 636 et RPC/135, NETBIOS/1 37-139 ne doit pas être autorisé depuis l'extérie ur du VPC via des groupes de sécurité.
8.0	L'accès à la gestion de base de données sur les ports (MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433) ou sur un port personnalisé ne doit pas être autorisé depuis un port public non routé vers un VPC via DX, VPC-Peer ou VPN via un groupe de sécurité. IPs
8.1	Toute ressource dans laquelle les données des clients peuvent être stockées ne doit pas être directement exposée à l'Internet public.

ID	Norme technique
9.0	L'accès direct aux applications via les ports HTTP/80, HTTPS/8443 et HTTPS/443 depuis Internet n'est autorisé qu'aux équilibreurs de charge, mais pas directement aux ressource s de calcul, par exemple les instances, les conteneurs, etc. EC2 ECS/EKS/Fargate
10,0	L'accès aux applications via les ports HTTP/80 et HTTPS/443 depuis la plage d'adresses IP privées du client peut être autorisé.
11,0	Toute modification des groupes de sécurité contrôlant l'accès à l'infrastructure AMS ne doit pas être autorisée sans acceptation des risques.
12,0	AMS Security fera référence aux normes chaque fois qu'il sera demandé d'associer un groupe de sécurité à une instance.
14,0	L'association VPCs entre comptes de zones hébergées privées avec un compte AMS vers un compte non-AMS (ou un compte non-AMS vers AMS) doit être configurée uniquement si le compte non-AMS appartient au même client AMS (en confirmant qu'il appartient au même compte d'organisation AWS ou en faisant correspondre le domaine de messagerie au nom de l'entreprise du client) à l'aide d'outils internes.
15,0	Les connexions de peering VPC entre des comptes appartenant au même client peuvent être autorisées.

ID	Norme technique
16,0	La base AMS AMIs peut être partagée avec un compte non-AMS à condition que les deux comptes appartiennent au même client (en confirmant qu'ils appartiennent au même AWS Organizations compte ou en faisant correspon dre le domaine de messagerie au nom de l'entreprise du client) à l'aide d'outils internes.
17,0	Le port FTP 21 ne doit être configuré dans aucun des groupes de sécurité sans acceptati on de risque.
18,0	La connectivité réseau entre comptes via une passerelle de transit est autorisée tant que tous les comptes appartiennent au client.
19,0	Il n'est pas permis de rendre public un sous-réseau privé
20.0	Les connexions de peering VPC avec des comptes tiers (n'appartenant pas au client) ne doivent pas être autorisées.
21,0	L'attachement de Transit Gateway à un compte tiers (n'appartenant pas au client) ne doit pas être autorisé.
22,0	Tout trafic réseau nécessaire à AMS pour fournir les services aux clients ne doit pas être bloqué au point de sortie du réseau du client.
23,0	Les demandes ICMP entrantes adressées EC2 à Amazon par le client infra nécessiteront une notification des risques.

ID	Norme technique
24,0	Les demandes entrantes provenant du public IPs acheminées vers Amazon VPC via DX, VPC-Peer ou VPN via un groupe de sécurité sont autorisées.
25.0	Les demandes entrantes émanant du public qui ne sont IPs pas acheminées vers Amazon VPC via DX, VPC-Peer ou VPN via un groupe de sécurité nécessiteraient une acceptation des risques.
26,0	Les demandes ICMP sortantes d'Amazon EC2 vers n'importe quelle destination sont autorisée s.
27,0	Partage de groupes de sécurité
27.1	Si un groupe de sécurité répond à cette norme de sécurité, il peut être partagé entre VPCs les comptes du même compte et entre les comptes de la même organisation.
27,2	Si un groupe de sécurité ne répond pas à cette norme et qu'une acceptation des risques était auparavant requise pour ce groupe de sécurité, l'utilisation de la fonctionnalité de partage de groupes de sécurité entre VPCs un même compte, ou entre des comptes d'une même organisation, n'est pas autorisée sans acceptation des risques pour ce nouveau VPC ou compte.

AMS-STD-X004 - Test de pénétration

Voici le contrôle standard pour X004 - Test de pénétration

1. AMS ne prend pas en charge l'infrastructure Pentest. C'est la responsabilité du client. Par exemple, Kali n'est pas une distribution Linux prise en charge par AMS.
2. Les clients doivent respecter les tests de pénétration.
3. AMS sera préinformée 24 heures à l'avance dans le cas où le client souhaiterait effectuer des tests de pénétration de l'infrastructure au sein de ses comptes.
4. AMS fournira une infrastructure de pentesting au client conformément aux exigences du client explicitement énoncées dans la demande de modification ou de service du client.
5. La gestion des identités pour l'infrastructure de pentesting des clients relève de la responsabilité du client.

AMS-STD-X005 - GuardDuty

La commande standard pour X005 est la suivante : GuardDuty

1. GuardDuty doit être activé dans tous les comptes clients à tout moment.
2. GuardDuty les alertes doivent être stockées dans le même compte ou dans tout autre compte géré par la même organisation.
3. La fonctionnalité de liste d'adresses IP fiables de ne GuardDuty doit pas être utilisée. L'archivage automatique peut plutôt être utilisé comme alternative, ce qui est utile à des fins d'audit.

AMS-STD-X007 - Journalisation

Voici le contrôle standard pour X007 - Logging

ID	Norme technique
1.0	Types de journaux
1.1	Journaux du système d'exploitation : tous les hôtes doivent enregistrer au minimum les événements d'authentification de l'hôte, les événements d'accès pour toutes les utilisati ons de privilèges élevés et les événements d'accès pour toutes les modifications apportées à l'accès et à la configuration des privilèges, y compris les réussites et les échecs.

ID	Norme technique
1.2	AWS CloudTrail: CloudTrail la journalisation des événements de gestion doit être activée et configurée pour transmettre les journaux à un compartiment S3.
1.3	Journaux de flux VPC : Tous les journaux de trafic réseau doivent être enregistrés via des journaux de flux VPC.
1.4	Journalisation de l'accès au serveur Amazon S3 : les compartiments S3 mandatés par AMS qui stockent les journaux doivent avoir la journalisation des accès au serveur activée.
1.5	AWS Config Instantanés : vous AWS Config devez enregistrer les modifications de configuration pour toutes les ressources prises en charge dans toutes les régions et transmettre les fichiers d'instantanés de configuration aux compartiments S3 au moins une fois par jour.
1,7	Journaux d'applications : les clients sont autorisés à activer la journalisation dans leurs applications et à les stocker dans un groupe de CloudWatch journaux ou un compartiment S3.
1.8	Journalisation au niveau de l'objet S3 : les clients sont autorisés à activer la journalisation au niveau de l'objet dans leurs compartiments S3.
1.9	Journalisation des services : les clients sont habilités à activer et à transférer les journaux pour les services SSPS, comme pour tous les services de base.

ID	Norme technique
1.10	Journaux Elastic Classic/Application Load Balancer/Network Load Balancing (Load Balancer) : les entrées du journal d'accès et d'erreurs doivent être stockées dans les compartiments S3 gérés par AMS 2.0.
2.0	Contrôle d'accès
2.3	Les compartiments S3 mandatés par AMS qui stockent les journaux ne doivent pas autoriser les utilisateurs de comptes tiers en tant que principe dans les politiques des compartiments.
2,4	Les CloudWatch journaux des groupes de journaux ne doivent pas être supprimés sans l'approbation explicite du contact de sécurité autorisé du client.
3,0	Conservation des journaux
3.1	Les groupes de CloudWatch journaux mandatés par AMS doivent avoir une période de conservation minimale de 90 jours pour les journaux.
3.2	Les compartiments S3 mandatés par AMS qui stockent les journaux doivent avoir une période de conservation minimale de 18 mois pour les journaux.
3.3	AWS Backup les instantanés doivent être disponibles avec une durée de conservation minimale de 31 jours sur les ressources prises en charge.
4,0	Chiffrement

ID	Norme technique
4.1	Le chiffrement doit être activé dans tous les compartiments S3 requis par AMS Teams qui stocke les journaux.
4.2	Tout transfert de journal d'un compte client vers un autre compte doit être crypté.
5,0	Intégrité
5.1	Le mécanisme d'intégrité du fichier journal doit être activé. Cela signifie configurer la « validatio n du fichier journal » dans les AWS CloudTrail pistes requises par les équipes AMS.
6.0	Transfert de journaux
6.1	Tout journal peut être transféré d'un compte AMS à un autre compte AMS du même client.
6.2	Tout journal peut être transféré d'un compte AMS vers un compte non-AMS uniquement si le compte non-AMS appartient au même client AMS (en confirmant qu'il appartient au même AWS Organizations compte ou en faisant correspondre le domaine de messagerie au nom de l'entreprise du client et au compte lié à PAYER) à l'aide d'outils internes.

Changements qui introduisent des risques de sécurité élevés ou très élevés dans votre environnement

Les modifications suivantes présentent un risque de sécurité élevé ou très élevé dans votre environnement :

AWS Identity and Access Management

- High_Risk-IAM-001 : Création de clés d'accès pour le compte root
- High_Risk-IAM-002 : Modification de la politique SCP pour autoriser un accès supplémentaire
- High_Risk-IAM-003 : modification de la politique SCP susceptible de perturber l'infrastructure AMS
- High_Risk-IAM-004 : Création d'une infrastructure role/user avec modification des autorisations (écriture, gestion des autorisations ou balisage) dans le compte client
- High_Risk-IAM-005 : Les rôles IAM font confiance aux politiques entre les comptes AMS et les comptes tiers (non détenus par le client)
- High_Risk-IAM-006 : Politiques entre comptes (permettant à un compte tiers d'accéder à n'importe quelle clé KMS depuis un compte AMS)
- High_Risk-IAM-007 : politiques inter-comptes appliquées par des comptes tiers pour accéder au compartiment S3 d'un client AMS ou à des ressources où les données peuvent être stockées (Amazon RDS, Amazon DynamoDB ou Amazon Redshift, par exemple)
- High_Risk-IAM-008 : Attribuez les autorisations IAM à toute autorisation modifiant l'infrastructure dans le compte client
- High_Risk-IAM-009 : Autoriser le listage et la lecture de tous les compartiments S3 du compte

Sécurité du réseau

- High_Risk-Net-001 : ports de gestion du système d'exploitation ouverts SSH/22 ou SSH/2222 (pas SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/CITRIX/1494 ou 1604, LDAP/389 ou 636 et NETBIOS/137-139 depuis Internet
- High_RISK-NET-002 : ports de gestion de base de données ouverts MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433 ou tout port client de gestion depuis Internet
- High_Risk-Net-003 : Ouvrez les ports d'application HTTP/80, HTTPS/8443 et HTTPS/443 directement sur toutes les ressources informatiques. Par exemple, EC2 des instances, ECS/EKS/ Fargate des conteneurs, etc. provenant d'Internet
- High_Risk-Net-004 : Toute modification apportée aux groupes de sécurité contrôlant l'accès à l'infrastructure AMS
- High_Risk-Net-006 : peering VPC avec le compte tiers (non détenu par le client)
- High_Risk-Net-007 : Ajout d'un pare-feu client comme point de sortie pour tout le trafic AMS
- High_Risk-Net-008 : La connexion Transit Gateway au compte tiers n'est pas autorisée
- High_Risk-S3-001 : Fournir ou activer l'accès public dans le compartiment S3

Journalisation

- High_Risk-Log-001 : Désactiver. CloudTrail
- High_Risk-Log-002 : Désactive les journaux de flux VPC.
- High_Risk-log-003 : transfert du journal via n'importe quelle méthode (notification d'événement S3, extraction de l'agent SIEM, push de l'agent SIEM, etc.) d'un compte géré par AMS vers un compte tiers (non détenu par le client)
- High_Risk-Log-004 : Utiliser une trace autre qu'AMS pour CloudTrail

Miscellaneous

- High_Risk-enc-001 : Désactive le chiffrement dans n'importe quelle ressource s'il est activé

FAQ sur la sécurité

AMS fournit une follow-the-sun assistance 24 heures sur 24, 7 jours sur 7 et 365 jours par an via des centres d'opérations Des ingénieurs opérationnels AMS dédiés surveillent activement les tableaux de bord et les files d'attente d'incidents. En général, AMS gère vos comptes par le biais de l'automatisation. Dans de rares circonstances nécessitant une expertise spécifique en matière de dépannage ou de déploiement, un ingénieur des opérations AMS peut accéder à vos AWS comptes.

Les questions suivantes sont fréquemment posées sur les meilleures pratiques de sécurité, les contrôles, les modèles d'accès et les mécanismes d'audit utilisés par AMS Accelerate lorsqu'un ingénieur des opérations ou un automate AMS accède à vos comptes.

Quand les ingénieurs opérationnels d'AMS accèdent-ils à mes environnements ?

Les ingénieurs opérationnels d'AMS n'ont pas un accès permanent à vos comptes ou instances. L'accès aux comptes clients est accordé aux opérateurs AMS uniquement pour des cas d'utilisation commerciale justifiables, tels que les alertes, les incidents, les demandes de modification, etc. L'accès est documenté dans AWS CloudTrail des journaux.

Pour la justification de l'accès, les déclencheurs et les initiateurs de déclencheurs, voirDéclencheurs d'accès au compte client AMS.

Quels sont les rôles des ingénieurs d'exploitation AMS lorsqu'ils accèdent à mes comptes ?

Dans les rares cas (~ 5 %) qui nécessitent une intervention humaine dans votre environnement, les ingénieurs opérationnels d'AMS se connectent à votre compte avec un rôle d'accès par défaut en lecture seule. Le rôle par défaut n'a accès à aucun contenu couramment stocké dans des magasins de données, tels qu'Amazon Simple Storage Service, Amazon Relational Database Service, Amazon DynamoDB, Amazon Redshift et Amazon. ElastiCache

Pour obtenir la liste des rôles dont les ingénieurs d'exploitation et les systèmes AMS ont besoin pour fournir des services dans votre compte, consultezAccès au compte client AMS | Rôles IAM.

Comment un ingénieur des opérations AMS accède-t-il à mon compte ?

Pour accéder aux comptes clients, les ingénieurs opérationnels d'AMS utilisent un service d'accès AMS AWS interne. Ce service interne n'est disponible que par le biais d'un canal privé sécurisé afin que l'accès à vos comptes soit sécurisé et audité.

1. Les ingénieurs opérationnels d'AMS utilisent l'authentification interne du service d'accès AMS ainsi qu'une authentification à deux facteurs. De plus, l'ingénieur des opérations doit fournir une justification commerciale (ticket d'incident ou numéro de demande de service) expliquant la nécessité d'accéder à votre AWS compte.
2. Sur la base de l'autorisation de l'ingénieur des opérations, le service d'accès AMS fournit à l'ingénieur le rôle approprié (Read-only/Operator/Admin) et l'URL de connexion à votre AWS console. L'accès à votre compte est de courte durée et limité dans le temps.
3. Pour accéder aux EC2 instances Amazon, les ingénieurs opérationnels d'AMS utilisent le même service d'accès AMS interne que le courtier. Une fois l'accès accordé, les ingénieurs d'exploitation AMS peuvent accéder AWS Systems Manager Session Manager à vos instances avec des informations d'identification de session de courte durée.

   Pour fournir un accès RDP aux instances Windows, l'ingénieur des opérations utilise Amazon EC2 Systems Manager pour créer un utilisateur local sur l'instance et établir une redirection de port vers l'instance. L'ingénieur des opérations utilise les informations d'identification de l'utilisateur local pour l'accès RDP à l'instance. Les informations d'identification de l'utilisateur local sont supprimées à la fin de la session.

Le schéma suivant décrit le processus utilisé par les ingénieurs d'exploitation d'AMS pour accéder à votre compte :

Comment suivre les modifications apportées par AMS dans mes AWS comptes gérés par AMS ?

Accès au compte

Pour vous aider à suivre les modifications apportées par l'automatisation ou par l'équipe opérationnelle d'AMS Accelerate, AMS fournit l'interface SQL Change record dans la console Amazon Athena et les journaux AMS Accelerate. Ces ressources fournissent les informations suivantes :

- Qui a accédé à votre compte.
- Quand le compte a été consulté.
- Quels privilèges ont été utilisés pour accéder à votre compte.
- Quelles modifications ont été apportées par AMS Accelerate à votre compte ?
- Pourquoi les modifications ont été apportées à votre compte.

Configuration des ressources

Consultez CloudTrail les journaux pour suivre les configurations de vos AWS ressources au cours des 90 derniers jours. Si votre configuration date de plus de 90 jours, accédez aux journaux dans Amazon S3.

Journaux d'instance

L' CloudWatch agent Amazon collecte les journaux du système d'exploitation. Consultez les CloudWatch journaux pour voir les journaux de connexion et les autres journaux d'actions pris en charge par votre système d'exploitation.

Pour de plus amples informations, veuillez consulter Suivi des modifications apportées à vos comptes AMS Accelerate.

Quels sont les contrôles de processus permettant à l'ingénieur des opérations AMS d'accéder à mon compte ?

Avant de rejoindre AMS, les ingénieurs des opérations sont soumis à une vérification de leurs antécédents criminels. Dans la mesure où les ingénieurs d'AMS gèrent l'infrastructure des clients, ils sont également soumis à une vérification annuelle obligatoire de leurs antécédents. Si un ingénieur échoue à la vérification des antécédents, l'accès est révoqué.

Tous les ingénieurs opérationnels d'AMS doivent suivre une formation de sécurité obligatoire, telle que la sécurité de l'infrastructure, la sécurité des données et la réponse aux incidents avant de pouvoir accéder aux ressources.

Comment sont gérés les accès privilégiés ?

Un sous-ensemble d'utilisateurs doit suivre une formation supplémentaire et conserver des droits d'accès privilégiés pour un accès élevé. L'accès et l'utilisation sont inspectés et audités. AMS limite l'accès privilégié à des circonstances exceptionnelles ou lorsque l'accès au moindre privilège ne permet pas de répondre à votre demande. L'accès privilégié est également limité dans le temps.

Les ingénieurs d'exploitation d'AMS utilisent-ils le MFA ?

Oui. Tous les utilisateurs doivent utiliser le MFA et la preuve de présence pour vous fournir des services.

Qu'advient-il de leur accès lorsqu'un employé d'AMS quitte l'organisation ou change de rôle ?

L'accès aux comptes et aux ressources des clients est fourni par le biais de l'adhésion à un groupe interne. L'adhésion est basée sur des critères stricts, notamment le rôle professionnel spécifique, le responsable des rapports et le statut professionnel chez AMS. Si la famille de tâches d'un ingénieur des opérations change ou si son nom d'utilisateur est désactivé, l'accès est révoqué.

Quels contrôles d'accès régissent l'accès des ingénieurs d'exploitation AMS à mes comptes ?

Il existe plusieurs niveaux de contrôles techniques pour appliquer les principes du « besoin de savoir » et du « moindre privilège » en matière d'accès à votre environnement. Voici une liste des contrôles d'accès :

- Tous les ingénieurs d'exploitation doivent faire partie d'un AWS groupe interne spécifique pour accéder aux comptes et aux ressources des clients. L'adhésion à un groupe est strictement basée sur le besoin de savoir et est automatisée selon des critères prédéfinis.
- AMS pratique un accès « non persistant » à votre environnement. Cela signifie que l'accès à vos AWS comptes par les opérations AMS se fait « just-in-time » avec des informations d'identification de courte durée. L'accès à vos comptes n'est accordé qu'après qu'une justification de l'analyse de rentabilisation interne (demande de service, incident, demande de gestion des modifications, etc.) a été soumise et examinée.
- AMS applique le principe du moindre privilège. Par conséquent, les ingénieurs d'exploitation autorisés supposent un accès en lecture seule par défaut. L'accès en écriture n'est utilisé par les ingénieurs que lorsque des modifications de votre environnement sont nécessaires en raison d'un incident ou d'une demande de modification.
- AMS utilise des AWS Identity and Access Management rôles standard facilement identifiables qui utilisent le préfixe « ams » pour surveiller et gérer vos comptes. Tous les accès sont enregistrés AWS CloudTrail pour que vous puissiez les auditer.
- AMS utilise des outils de backend automatisés pour détecter les modifications non autorisées apportées à votre compte pendant la phase de validation des informations client lors de l'exécution des modifications.

Comment AMS surveille-t-il l'accès des utilisateurs root ?

L'accès root déclenche toujours le processus de réponse aux incidents. AMS utilise le système GuardDuty de détection Amazon pour surveiller l'activité de l'utilisateur root. S'il GuardDuty génère une alerte, AMS crée un événement pour une enquête plus approfondie. AMS vous avertit si une activité inattendue du compte root est détectée, et l'équipe de sécurité AMS lance une enquête.

Comment l'AMS réagit-il aux incidents de sécurité ?

AMS enquête sur les événements de sécurité générés par des services de détection tels qu'Amazon GuardDuty, Amazon Macie, et par des problèmes de sécurité signalés par des clients. AMS collabore avec votre équipe d'intervention en matière de sécurité pour exécuter le processus de réponse aux incidents de sécurité (SIR). Le processus AMS SIR est basé sur le framework NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide, et fournit une réponse de sécurité 24 follow-the-sun heures sur 24, 7 jours sur 7, 365 jours par an. AMS travaille avec vous pour analyser et contenir rapidement les incidents de sécurité.

Quels sont les cadres et certifications standard du secteur auxquels AMS adhère ?

Comme les autres AWS services, AWS Managed Services est certifié OSPAR, HIPAA, HITRUST, RGPD, SOC*, ISO*, FedRAMP (Medium/High), IRAP et PCI. Pour plus d'informations sur les certifications de conformité des clients, les réglementations et les cadres qui AWS s'y conforment, consultez la section Conformité AWS.

Rambardes de sécurité

AWS Managed Services utilise de multiples contrôles pour protéger vos actifs informationnels et vous aider à garantir la sécurité de votre AWS infrastructure. AMS Accelerate gère une bibliothèque de AWS Config règles et d'actions correctives pour vous aider à vous assurer que vos comptes sont conformes aux normes du secteur en matière de sécurité et d'intégrité opérationnelle. AWS Config les règles suivent en permanence les modifications de configuration sur vos ressources enregistrées. Si une modification enfreint les conditions d'une règle, AMS vous fait part de ses conclusions. Vous pouvez corriger les violations automatiquement ou sur demande, en fonction de la gravité de la violation.

AMS utilise des AWS Config règles pour répondre aux exigences des normes suivantes :

- Centre pour la sécurité Internet (CIS)
- Cadre de sécurité cloud (CSF) du National Institute of Standards and Technology (NIST)
- Health Insurance Portability and Accountability Act (HIPAA)
- Norme de sécurité des données (DSS) de l'industrie des cartes de paiement (PCI)

Pour de plus amples informations, consultez Gestion de la sécurité dans AMS Accelerate.

Comment puis-je accéder aux derniers rapports sur la certification de sécurité, les cadres et la conformité AWS ?

Vous pouvez accéder aux rapports de sécurité et de conformité actuels pour les AWS services en utilisant les méthodes suivantes :

- Vous pouvez l'utiliser AWS Artifactpour télécharger le dernier rapport sur la sécurité, la disponibilité et la confidentialité d'un AWS service.

- Pour obtenir une liste de la plupart AWS des services, y compris AWS Managed Services, qui sont conformes aux cadres de conformité mondiaux, consultezhttps://aws.amazon.com/compliance/services-in-scope/. Par exemple, sélectionnez PCI et recherchez AWS Managed Services.

  Vous pouvez rechercher « AMS » pour trouver des artefacts de sécurité spécifiques à AMS provenant d'un AWS compte géré par AMS. AWS Managed Services est concerné par le SOC 3.
- Le rapport AWS SOC 2 (System and Organizations Controls) est publié dans le AWS Artifact référentiel. Ce rapport évalue les AWS contrôles qui répondent aux critères de sécurité, de disponibilité et de confidentialité énoncés dans la section 100 du TSP de l'American Institute of Certified Public Accountants (AICPA), intitulée Trust Services Criteria.

AMS partage-t-il des diagrammes d'architecture de référence illustrant les différents aspects des fonctionnalités d'AMS ?

Pour consulter l'architecture de référence AMS, téléchargez le PDF AWS Managed Services for Proactive Monitoring.

Comment AMS vérifie-t-elle qui accède à mes comptes et quels sont les besoins de l'entreprise en matière d'accès ?

Pour garantir la continuité du service et la sécurité de vos comptes, AMS accède à votre compte ou à vos instances uniquement en réponse à des problèmes de santé ou de maintenance proactifs, à des événements liés à la santé ou à la sécurité, à des activités planifiées ou à des demandes des clients. L'accès à vos comptes est autorisé par le biais des processus AMS tels que décrits dans le modèle d'accès d'AMS Accelerate. Ces flux d'autorisation contiennent des barrières de sécurité pour empêcher tout accès accidentel ou inapproprié. Dans le cadre du flux d'accès, AMS fournit au système d'autorisation un besoin commercial. Ce besoin professionnel peut être un élément de travail associé à votre compte, tel qu'un dossier que vous avez ouvert auprès d'AMS. L'entreprise peut également avoir besoin d'un flux de travail autorisé, tel que la solution d'application de correctifs. Tout accès nécessite une justification validée, vérifiée et autorisée en temps réel par les systèmes AMS internes sur la base de règles métier afin d'aligner les demandes d'accès sur les besoins de l'entreprise.

Les ingénieurs opérationnels d'AMS ne sont pas autorisés à accéder à vos comptes s'ils ne répondent pas à des besoins commerciaux valides. Tous les accès aux comptes et les besoins commerciaux associés sont AWS CloudTrail enregistrés dans vos AWS comptes. Cela garantit une transparence totale et vous donne la possibilité d'effectuer vos propres audits et inspections. Outre

votre inspection, AMS effectue des inspections automatisées et effectue une inspection manuelle des demandes d'accès, selon les besoins, et réalise des audits de l'outillage et de l'accès humain pour examiner les accès anormaux.

Les ingénieurs d'AMS ont-ils accès à mes données stockées dans un service de stockage de AWS données, tel qu'Amazon S3, Amazon RDS, DynamoDB et Amazon Redshift ?

Les ingénieurs d'AMS n'ont pas accès au contenu client stocké dans les AWS services couramment utilisés pour le stockage de données. L'accès aux données AWS APIs utilisées pour lire, écrire, modifier ou supprimer des données dans ces services est limité par une politique de refus IAM explicite associée aux rôles IAM utilisés pour l'accès des ingénieurs AMS. En outre, les garde-fous internes et les automatisations de l'AMS empêchent les ingénieurs d'exploitation d'AMS de supprimer ou de modifier les conditions de refus.

Les ingénieurs d'AMS ont-ils accès aux données clients stockées dans Amazon EBS, Amazon EFS et Amazon FSx ?

Les ingénieurs AMS peuvent se connecter aux EC2 instances Amazon en tant qu'administrateurs. L'accès de l'administrateur est requis pour la correction dans certains scénarios qui incluent, sans toutefois s'y limiter, les problèmes liés au système d'exploitation (OS) et les défaillances de correctifs. Les ingénieurs AMS accèdent généralement au volume du système pour résoudre les problèmes détectés. Cependant, l'accès pour les ingénieurs d'AMS n'est ni limité ni limité au volume du système.

Comment l'accès est-il restreint ou contrôlé pour les rôles d'automatisation dotés de privilèges élevés pour mes environnements ?

Le `ams-access-admin` rôle est utilisé exclusivement par AMS Automation. Ces automatisations déploient, gèrent et maintiennent les ressources requises utilisées par AMS pour les déployer dans vos environnements pour la collecte de données de télémétrie, de santé et de sécurité afin d'exécuter des fonctions opérationnelles. Les ingénieurs AMS ne peuvent pas assumer de rôles d'automatisation et sont limités par le mappage des rôles dans les systèmes internes. Au moment de l'exécution, AMS applique dynamiquement une politique de session avec le moindre privilège à chaque automatisation. Cette politique de session limite les capacités et les autorisations de l'automatisation.

Comment AMS met-il en œuvre le principe du moindre privilège tel que préconisé dans le AWS Well-Architected Framework pour les rôles d'automatisation ?

Au moment de l'exécution, AMS applique une politique de session limitée, avec le moindre privilège, à chaque automatisation. Cette politique de session limitée limite les capacités et les autorisations de l'automatisation. Les politiques de session qui disposent des autorisations nécessaires pour créer des ressources IAM doivent également associer une limite d'autorisation. Cette limite d'autorisation réduit le risque d'augmentation des privilèges. Chaque équipe adopte une politique de session qui n'est utilisée que par cette équipe.

Quels sont les systèmes de journalisation et de surveillance utilisés pour détecter les tentatives d'accès non autorisées ou les activités suspectes impliquant des rôles d'automatisation ?

AWS gère des référentiels centralisés qui fournissent des fonctionnalités essentielles d'archivage des journaux à usage interne par les équipes de AWS service. Ces journaux sont stockés dans Amazon S3 pour garantir une évolutivité, une durabilité et une disponibilité optimales. AWS les équipes de service peuvent ensuite collecter, archiver et consulter les journaux de service dans un service de journal central.

Les hôtes de production AWS sont déployés à l'aide d'images de référence principales. Les images de référence sont équipées d'un ensemble standard de configurations et de fonctions qui incluent la journalisation et la surveillance à des fins de sécurité. Ces journaux sont stockés et accessibles par les équipes AWS de sécurité à des fins d'analyse des causes premières en cas d'incident de sécurité suspect.

Les journaux d'un hôte donné sont accessibles à l'équipe propriétaire de cet hôte. Les équipes peuvent consulter leurs journaux à des fins d'analyse opérationnelle et de sécurité.

Comment sont gérés les incidents ou violations de sécurité concernant l'infrastructure d'automatisation, et quels protocoles contribuent à une réponse et à une atténuation rapides ?

AWS les plans d'urgence et les manuels de réponse aux incidents ont défini et testé des outils et des processus pour détecter, atténuer, étudier et évaluer les incidents de sécurité. Ces

plans et playbooks incluent des directives pour répondre aux violations de données potentielles conformément aux exigences contractuelles et réglementaires.

Des évaluations de sécurité, des analyses de vulnérabilité et des tests de pénétration sont-ils régulièrement effectués sur l'infrastructure d'automatisation ?

AWS Security analyse régulièrement les vulnérabilités des systèmes d'exploitation hôtes, des applications Web et des bases de données de l' AWS environnement à l'aide de divers outils. AWS Les équipes de sécurité s'abonnent également aux fils d'actualités pour détecter les failles applicables aux fournisseurs et surveillent de manière proactive les sites Web des fournisseurs et les autres points de vente pertinents pour détecter les nouveaux correctifs.

Comment l'accès à l'infrastructure d'automatisation est-il limité au personnel autorisé uniquement ?

L'accès aux AWS systèmes est attribué en fonction du moindre privilège et approuvé par une personne autorisée. Les tâches et les domaines de responsabilité (par exemple, la demande et l'approbation d'accès, la demande et l'approbation de la gestion des modifications, le développement des modifications, les tests et le déploiement, etc.) sont répartis entre différentes personnes afin de réduire les modifications non autorisées ou involontaires ou l'utilisation abusive des systèmes. AWS Les comptes de groupe ou partagés ne sont pas autorisés dans les limites du système.

Quelles sont les mesures mises en œuvre pour respecter les normes de sécurité et empêcher les accès non autorisés ou les violations de données dans le pipeline d'automatisation ?

L'accès aux ressources, notamment aux services, aux hôtes, aux périphériques réseau et aux groupes Windows et UNIX, est approuvé dans le système de gestion des autorisations AWS propriétaire par le propriétaire ou le responsable approprié. Le journal de l'outil de gestion des autorisations enregistre les demandes de modification d'accès. Les modifications apportées aux fonctions du poste révoquent automatiquement l'accès de l'employé aux ressources. L'accès continu pour cet employé doit être demandé et approuvé.

AWS nécessite une authentification à deux facteurs via un canal cryptographique approuvé pour l'authentification sur le AWS réseau interne à partir de sites distants. Les dispositifs pare-feu

limitent l'accès à l'environnement informatique, renforcent les limites des clusters informatiques et restreignent l'accès aux réseaux de production.

Des processus sont mis en œuvre pour protéger les informations d'audit et les outils d'audit contre tout accès, modification et suppression non autorisés. Les dossiers d'audit contiennent un ensemble d'éléments de données destinés à répondre aux exigences d'analyse nécessaires. En outre, les enregistrements d'audit sont mis à la disposition des utilisateurs autorisés à des fins d'inspection ou d'analyse à la demande, et en réponse à des événements liés à la sécurité ou ayant un impact sur l'activité.

Les droits d'accès des utilisateurs aux AWS systèmes (par exemple, au réseau, aux applications, aux outils, etc.) sont révoqués dans les 24 heures suivant la résiliation ou la désactivation. Les comptes utilisateurs inactifs sont désactivés et and/or supprimés au moins tous les 90 jours.

La détection ou la surveillance des anomalies sont-elles activées pour les accès ou la journalisation des audits pour détecter l'augmentation des privilèges ou les abus d'accès afin d'alerter de manière proactive l'équipe AMS ?

Les hôtes de production de AWS sont équipés d'un système de journalisation pour des raisons de sécurité. Ce service enregistre les actions humaines sur les hôtes, y compris les connexions, les tentatives d'ouverture de session infructueuses et les fermetures de session. Ces journaux sont stockés et accessibles par les équipes AWS de sécurité à des fins d'analyse des causes premières en cas d'incident de sécurité suspect. Les journaux d'un hôte donné sont également accessibles à l'équipe propriétaire de cet hôte. Un outil d'analyse des journaux frontal est à la disposition des équipes de service qui souhaitent consulter leurs journaux à des fins d'analyse opérationnelle et de sécurité. Des processus sont mis en œuvre pour protéger les journaux et les outils d'audit contre tout accès, modification et suppression non autorisés. L'équipe AWS de sécurité effectue une analyse des journaux pour identifier les événements en fonction de paramètres de gestion des risques définis.

Quels types de données clients sont extraits des comptes gérés par AMS, et comment sont-ils utilisés et stockés ?

AMS n'accède à votre contenu ni ne l'utilise à quelque fin que ce soit. AMS définit le contenu client comme un logiciel (y compris des images de machine), des données, du texte, du son, de la vidéo ou des images vers lesquels un client ou un utilisateur final transfère à des AWS fins de traitement, de stockage ou d'hébergement Services AWS en lien avec le compte d'un client, ainsi que tout résultat

de calcul qu'un client ou son utilisateur final obtient de ce qui précède en utilisant ce qui précède. Services AWS

Surveillance et gestion des événements dans AMS Accelerate

Le système de surveillance AMS Accelerate surveille vos AWS ressources pour détecter les défaillances, la dégradation des performances et les problèmes de sécurité.

En tant que compte géré, AMS Accelerate configure et déploie des alarmes pour les AWS ressources applicables, surveille ces ressources et effectue des mesures correctives en cas de besoin.

Le système de surveillance AMS Accelerate repose sur des outils internes, tels que Resource Tagger et Alarm Manager, et sur des outils tels qu'AWS AppConfigAmazon CloudWatch (CloudWatch) Services AWS, Amazon EventBridge (anciennement connu sous le nom de CloudWatch) GuardDuty, Amazon, Amazon Macie et. AWS Health

AMS Accelerate fournit une gamme de services opérationnels pour vous aider à atteindre l'excellence opérationnelle sur AWS. Pour comprendre rapidement comment AMS aide vos équipes à atteindre l'excellence opérationnelle globale AWS Cloud grâce à certaines de nos principales fonctionnalités opérationnelles, notamment le service d'assistance 24 h/24, 7 j/7, la surveillance proactive, la sécurité, l'application de correctifs, la journalisation et la sauvegarde, consultez les diagrammes d'architecture de référence AMS.

Rubriques

- Qu'est-ce que le monitoring ?
- Fonctionnement de la surveillance
- Alertes issues de la surveillance de base dans AMS
- Notifications d'incidents liées aux applications dans AMS
- Accélérer Alarm Manager
- Correction automatique des alertes par AMS
- Utilisation des règles EventBridge gérées par Amazon dans AMS
- Remédiateur fiable dans AMS

Pour plus d'informations sur la surveillance d'Amazon EKS, consultez Surveillance et gestion des incidents pour Amazon EKS dans AMS Accelerate

Qu'est-ce que le monitoring ?

La surveillance AMS Accelerate offre les avantages suivants :

- Configuration par défaut qui crée, gère et déploie des politiques sur l'ensemble de votre compte géré pour toutes les ressources ou les AWS ressources prises en charge que vous sélectionnez.
- Une base de surveillance qui vous permet de disposer d'un niveau de protection par défaut, même si vous ne configurez aucune autre surveillance pour vos comptes gérés. Pour de plus amples informations, veuillez consulter Alertes issues de la surveillance de base dans AMS.
- Possibilité de personnaliser les alarmes relatives aux ressources de base en fonction de vos besoins.
- Correction automatique des alertes par AMS Operations, dans la mesure du possible, afin de prévenir ou de réduire l'impact sur vos applications. Par exemple, si vous utilisez une EC2 instance Amazon autonome et que celle-ci échoue au contrôle de santé du système, AMS tente de récupérer l'instance en l'arrêtant puis en la redémarrant. Pour plus d'informations, consultez Correction automatique des alertes par AMS.
- Visibilité des alertes actives et précédemment résolues à l'aide de OpsCenter. Par exemple, si le taux d'utilisation du processeur d'une EC2 instance Amazon est élevé de manière inattendue, vous pouvez demander l'accès à la AWS Systems Manager console (y compris l'accès à la OpsCenter console) et le consulter OpsItem directement dans la OpsCenter console.
- Enquêter sur les alertes afin de déterminer les actions appropriées. Pour de plus amples informations, veuillez consulter Gestion des incidents dans AMS Accelerate.
- Alertes générées en fonction de la configuration de votre compte et des AWS services pris en charge. La configuration de surveillance d'un compte fait référence à tous les paramètres de ressources du compte qui créent une alerte. La configuration de surveillance d'un compte inclut les définitions des CloudWatch alarmes et EventBridge (anciennement connues sous le nom d' CloudWatch événements) qui génèrent l'alerte (alarme ou événement). Pour plus d'informations sur les paramètres des ressources, consultezAlertes issues de la surveillance de base dans AMS.
- Notification de défaillances imminentes, en cours, en cours, en cours ou potentielles, d'une dégradation des performances ou de problèmes de sécurité générés par la surveillance de base configurée dans un compte (appelée alerte). Des exemples d'alertes incluent une CloudWatch alarme, un événement ou une découverte provenant d'un AWS service, tel que GuardDuty ou AWS Health.

Fonctionnement de la surveillance

Consultez les graphiques suivants sur l'architecture de surveillance dans AWS Managed Services (AMS).

Le schéma suivant décrit l'architecture de surveillance AMS Accelerate.

Une fois que vos ressources ont été étiquetées en fonction de la politique définie à l'aide de Resource Tagger et que les définitions d'alarme ont été déployées, la liste suivante décrit les processus de surveillance AMS.

- Génération : Au moment de l'intégration du compte, AMS configure la surveillance de base (combinaison d'alarmes CloudWatch (CW) et de règles relatives aux événements CW) pour toutes vos ressources créées dans un compte géré. La configuration de surveillance de base génère une alerte lorsqu'une alarme CW est déclenchée ou qu'un événement CW est généré.
- Agrégation : toutes les alertes générées par vos ressources sont envoyées au système de surveillance AMS en les dirigeant vers une rubrique SNS du compte. Vous pouvez également configurer la manière dont AMS regroupe les EC2 alertes Amazon. AMS regroupe toutes les alertes relatives à la même EC2 instance en un seul incident ou crée un incident par alerte, selon vos préférences. Vous pouvez modifier cette configuration à tout moment en travaillant avec votre responsable de prestation de services cloud ou votre architecte cloud.
- Traitement : AMS analyse les alertes et les traite en fonction de leur impact potentiel. Les alertes sont traitées comme décrit ci-dessous.
  - Alertes ayant un impact connu sur le client : elles mènent à la création d'un nouveau rapport d'incident et AMS suit le processus de gestion des incidents.

    Exemple d'alerte : une EC2 instance Amazon échoue à une vérification de l'état du système, AMS tente de récupérer l'instance en l'arrêtant puis en la redémarrant.
  - Alertes dont l'impact sur le client est incertain : pour ces types d'alertes, AMS envoie un rapport d'incident, vous demandant dans de nombreux cas de vérifier l'impact avant qu'AMS ne prenne des mesures. Toutefois, si les contrôles liés à l'infrastructure sont réussis, AMS ne vous envoie pas de rapport d'incident.

    Par exemple : une alerte signalant une utilisation du processeur supérieure à 85 % pendant plus de 10 minutes sur une EC2 instance Amazon ne peut pas être immédiatement considérée comme un incident, car ce comportement peut être attendu en fonction de l'utilisation. Dans

cet exemple, AMS Automation effectue des contrôles liés à l'infrastructure sur la ressource. Si ces contrôles sont réussis, AMS n'envoie pas de notification d'alerte, même si l'utilisation du processeur dépasse les 99 %. Si Automation détecte que les contrôles liés à l'infrastructure échouent sur la ressource, AMS envoie une notification d'alerte et vérifie si des mesures d'atténuation sont nécessaires. Les notifications d'alerte sont abordées en détail dans cette section. AMS propose des options d'atténuation dans la notification. Lorsque vous répondez à la notification confirmant que l'alerte est un incident, AMS crée un nouveau rapport d'incident et le processus de gestion des incidents AMS démarre. Les notifications de service qui reçoivent une réponse indiquant « aucune incidence sur le client », ou aucune réponse pendant trois jours, sont marquées comme résolues et l'alerte correspondante est marquée comme résolue.

- Alertes sans impact sur le client : si, après évaluation, AMS détermine que l'alerte n'a pas d'impact sur le client, l'alerte est fermée.

  Par exemple, AWS Health indique qu'une EC2 instance doit être remplacée mais que cette instance a depuis été résiliée.

EC2 notifications groupées par instances

Vous pouvez configurer la surveillance AMS pour regrouper les alertes provenant d'une même EC2 instance en un seul incident. Votre responsable de prestation de services cloud ou votre architecte cloud peuvent le configurer pour vous. Vous pouvez configurer quatre paramètres pour chaque compte géré par AMS.

1. Champ d'application : choisissez soit à l'échelle du compte, soit basé sur des balises.
   - Pour spécifier une configuration qui s'applique à chaque EC2 instance de ce compte, choisissez scope = account-wide.
   - Pour spécifier une configuration qui s'applique uniquement aux EC2 instances de ce compte dotées d'une balise spécifique, choisissez scope = tag-based.
2. Règle de regroupement : Choisissez classique ou instance.
   - Pour configurer le regroupement au niveau de l'instance pour chaque ressource de votre compte, choisissez scope = à l'échelle du compte et règle de regroupement = instance.
   - Pour configurer des ressources spécifiques de votre compte afin d'utiliser le regroupement au niveau des instances, balisez ces instances, puis choisissez scope = basé sur des balises et règle de regroupement = niveau d'instance.
   - Pour ne pas utiliser le regroupement d'instances pour les alertes de votre compte, choisissez la règle de regroupement = classique.

3. Option d'engagement : choisissez aucun, rapport uniquement ou par défaut.
   - Pour qu'AMS ne crée pas d'incidents ou n'exécute pas d'automatisations pour les alarmes provenant de ces ressources lorsque la configuration est active, choisissez aucun.
   - Pour qu'AMS ne crée pas d'incidents ou n'exécute pas d'automatisations pour les alarmes provenant de ces ressources lorsque la configuration est active, et qu'il n'exécute pas de documents de guérison automatique de Systems Manager, mais pour inclure des enregistrements de ces événements dans vos rapports, choisissez report only. Cela peut être utile si vous souhaitez réduire le volume de demandes d'assistance avec lesquelles vous interagissez et si certains incidents liés à certaines ressources ne nécessitent pas une attention immédiate, par exemple ceux liés à un compte hors production.
   - Pour qu'AMS puisse traiter vos alertes, exécuter des automatisations et créer des cas d'incident en cas de besoin, choisissez le paramètre par défaut.
4. Résoudre après : choisissez 24 heures, 48 heures ou 72 heures. Enfin, configurez le moment où les cas d'incidents sont automatiquement fermés. Si le délai écoulé depuis la dernière correspondance de cas atteint la valeur Resolve after configurée, l'incident est clos.

Notification d'alerte

Dans le cadre du traitement des alertes, sur la base de l'analyse d'impact, AWS Managed Services (AMS) crée un incident et lance le processus de gestion des incidents pour y remédier, lorsque l'impact peut être déterminé. Si l'impact ne peut être déterminé, AMS envoie une notification d'alerte à l'adresse e-mail associée à votre compte par le biais d'une notification de service. Dans certains scénarios, cette notification d'alerte n'est pas envoyée. Par exemple, si les vérifications liées à l'infrastructure aboutissent à une alerte d'utilisation élevée du processeur, aucune notification d'alerte ne vous est envoyée. Pour plus d'informations, consultez le schéma de l'architecture de surveillance AMS pour le processus de gestion des alertes dansFonctionnement de la surveillance.

Notification d'alerte basée sur des balises

Utilisez des balises pour envoyer des notifications d'alerte concernant vos ressources à différentes adresses e-mail. Il est recommandé d'utiliser des notifications d'alerte basées sur des balises, car les notifications envoyées à une seule adresse e-mail peuvent être source de confusion lorsque plusieurs équipes de développeurs utilisent le même compte. Les notifications d'alerte basées sur des balises ne sont pas affectées par les EC2 notifications groupées par instances paramètres que vous choisissez.

Grâce aux notifications d'alerte basées sur des balises, vous pouvez :

- Envoyer des alertes à une adresse e-mail spécifique : Marquez les ressources dont les alertes doivent être envoyées à une adresse e-mail spécifique avec le`key = OwnerTeamEmail`,`value = EMAIL_ADDRESS`.
- Envoyer des alertes à plusieurs adresses e-mail : pour utiliser plusieurs adresses e-mail, spécifiez une liste de valeurs séparées par des virgules. Par exemple, `key = OwnerTeamEmail`, `value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ...`. Le nombre total de caractères pour le champ de valeur ne peut pas dépasser 260.
- Utiliser une clé de balise personnalisée : pour utiliser une clé de balise personnalisée, fournissez le nom de la clé de balise personnalisée à votre CSDM dans un e-mail qui donne explicitement votre accord pour activer les notifications automatiques pour la communication basée sur des balises. Il est recommandé d'utiliser la même stratégie de balisage pour les balises de contact dans toutes vos instances et ressources.

> **Note**
>
> Il n'est `OwnerTeamEmail` pas nécessaire que la valeur clé soit dans Camel Case. Toutefois, les balises font la distinction majuscules/majuscules et il est recommandé d'utiliser le format recommandé.
> L'adresse e-mail doit être spécifiée dans son intégralité, avec le signe « at » (@) pour séparer la partie locale du domaine. Exemples d'adresses e-mail non valides : `Team.AppATabc.xyz` ou`john.doe`. Pour obtenir des conseils généraux sur votre stratégie de balisage, consultez la section Ressources relatives au balisage AWS. N'ajoutez pas d'informations personnelles identifiables (PII) dans vos tags. Utilisez des listes de distribution ou des alias dans la mesure du possible.
> Les notifications d'alerte basées sur des balises sont prises en charge pour les ressources des services Amazon suivants : Elastic Block Store (EBS) EC2, Elastic Load Balancing (ELB), Application Load Balancer (ALB), Network Load Balancer, Relational Database Service (RDS), Elastic File System (EFS) et VPN. OpenSearch FSx Site-to-Site

Alertes issues de la surveillance de base dans AMS

Découvrez les paramètres de surveillance par défaut d'AMS Accelerate. Pour de plus amples informations, veuillez consulter Surveillance et gestion des événements dans AMS Accelerate.

Le tableau suivant indique ce qui est surveillé et les seuils d'alerte par défaut. Vous pouvez modifier les seuils d'alerte à l'aide d'un document de configuration personnalisé ou envoyer une demande de service. Pour obtenir des instructions sur la modification de votre configuration d'alarme personnalisée, consultezModification de la configuration de l'alarme Accelerate. Pour recevoir des notifications lorsque les alarmes dépassent leur seuil, outre le processus d'alerte standard d'AMS, vous pouvez remplacer les configurations d'alarme. Pour obtenir des instructions, veuillez consulter Accélérer Alarm Manager.

Amazon CloudWatch assure une rétention prolongée des métriques. Pour plus d'informations, consultez Limites CloudWatch .

> **Note**
>
> AMS Accelerate calibre périodiquement sa surveillance de base. Les nouveaux comptes sont toujours intégrés avec le suivi de référence le plus récent et le tableau décrit le suivi de référence pour un compte nouvellement intégré. AMS Accelerate met régulièrement à jour la surveillance de base des comptes existants et il se peut que vous subissiez un certain délai avant que les mises à jour ne soient mises en place.

Alertes issues de la surveillance de base

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
Pour les alertes marquées d'un astérisque (*), AMS évalue l'impact de manière proactive et y remédie lorsque cela est possible ; si la correction n'est pas possible, AMS crée un incident. Lorsque l'automatisation ne permet pas de résoudre le problème, AMS vous informe du cas d'incident et un ingénieur AMS est engagé. De plus, si vous optez pour la rubrique Direct-Cu stomer-Alerts SNS, ces alertes sont envoyées directement à votre adresse e-mail.		
Instance d'Application Load Balancer	ApplicationLoadBalancerErro rCount (HTTPCode_ELB_5xx_Count/ RequestCount) *100 somme > 15 % pendant 1 min, 5 fois de suite.	Nombre d'erreurs LoadBalan cer HTTP 5XX de l'application CloudWatch alarme en cas de nombre excessif de codes de réponse HTTP 5XX générés par le Loadbalancer.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
Instance d'Application Load Balancer	RejectedConnectionCount somme > 0 % pendant 1 min, 5 fois de suite.	Nombre de connexions LoadBalancer rejetées par l'application CloudWatch alarme si le nombre de connexions rejetées parce que l'équilib reur de charge a atteint son maximum
Application Load Balancer cible	TargetConnectionErrorCount (HTTPCode_TARGET_5 xx_Count/RequestCount) *100 somme > 15 % pendant 1 min, 5 fois de suite.	$ {ElasticLoadBalancingV2 : : TargetGroup :FullName } - Nombre d'erreurs de connexion à la LoadBalan cer cible de l'application - $ {ElasticLoadBalancingV2 : TargetGroup : :UUID} CloudWatch alarme en cas de nombre excessif de codes de réponse HTTP 5XX générés par une cible.
Application Load Balancer cible	ApplicationLoadBalancerTarg etGroupErrorCount somme > 0 % pendant 1 min, 5 fois de suite.	$ {ElasticLoadBalancingV2 : : TargetGroup :FullName} - Nombre d'erreurs HTTP 5XX de l'application LoadBalancer cible - $ {ElasticLoadBalanc ingV2 : TargetGroup : :UUID} CloudWatch alarme si le nombre de connexions a été établi sans succès entre l'équilibreur de charge et les instances enregistrées.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
EC2 Instance Amazon : toutes OSs	CPUUtilization* > 95 % pendant 5 minutes, 6 fois de suite.	$ {EC2: :InstanceId} : CPU trop élevé CloudWatch alarme. L'utilisation élevée du processeur est un indicateur d'un changement d'état de l'application, tel que des blocages, des boucles infinies, des attaques malveillantes et d'autres anomalies. Ce sont des Direct-Customer-Alerts alarmes.
EC2 Instance Amazon : toutes OSs	StatusCheckFailed > 0 % pendant 5 minutes, 3 fois de suite.	$ {EC2: :InstanceId} : échec de la vérification du statut CloudWatch alarme. L'échec de la vérification du statut indique qu'une EC2 instance Amazon portant l'ID spécifié a échoué à une ou plusieurs de ses vérifications de statut automatisées. Cela signifie que l'instance rencontre un problème qui l'empêche de fonctionner correctement ou d'être accessible.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
EC2 Instance Amazon - Linux	Minimum mem_used_percent >= 95 % pendant 5 minutes, 6 fois de suite.	$ {EC2: :InstanceId} : mémoire libre CloudWatch alarme. Memory Free indique que la mémoire disponible (RAM) sur l' EC2 instance Amazon spécifiée est tombée en dessous d'un seuil défini. Cela peut entraîner des problèmes de mémoire, des pannes du système et indiquer que l'instance peut avoir besoin de plus de RAM. Ce sont des Direct-Customer-Alerts alarmes.
EC2 Instance Amazon - Linux	Swap_used_percent moyen >= 95 % pendant 5 minutes, 6 fois de suite.	$ {EC2: :InstanceId} : Swap gratuit CloudWatch alarme. La valeur moyenne de swap_used _percent sur une instance EC2 Amazon indique que le pourcentage moyen d'espace de swap alloué actuellem ent utilisé a dépassé un seuil prédéfini. Cela peut entraîner une dégradation des performances, des blocages et des problèmes de mémoire. Ce sont des Direct-Customer-Alerts alarmes.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
EC2 Instance Amazon - Linux	Pourcentage maximal d'utilisation du disque >= 95 % pendant 5 minutes, 6 fois de suite.	$ {EC2: :InstanceId} : Utilisation du disque trop élevée - $ {EC2: :Disk : :UUID} CloudWatch alarme. Une utilisation trop élevée du disque indique que l'utilisation du disque sur un Amazon spécifique EC2 ou sur le disque identifié est proche de sa capacité maximale. Cela peut entraîner une dégradation des performances, des erreurs d'application et une instabilité du système. Ce sont des Direct-Customer-Alerts alarmes.
EC2 Instance Amazon - Windows	% de mémoire minimale en octets engagés en cours d'utilisation >= 95 % pendant 5 minutes, 6 fois de suite.	$ {EC2: :InstanceId} : mémoire libre CloudWatch alarme. Memory Free indique que la mémoire disponible (RAM) sur l' EC2 instance Amazon spécifiée est tombée en dessous d'un seuil défini. Cela peut entraîner des problèmes de mémoire, des pannes du système et indiquer que l'instance peut avoir besoin de plus de RAM. Ce sont des Direct-Customer-Alerts alarmes.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
EC2 Instance Amazon - Windows	LogicalDisk % maximum d'espace libre <= 5 % pendant 5 minutes, 6 fois de suite.	$ {EC2: :InstanceId} : Utilisation du disque trop élevée - $ {EC2: :Disk : :UUID} CloudWatch alarme. Indique que le pourcentage d'espace libre sur un disque logique (une partition de système de fichiers) au sein d'une instance Amazon EC2 Windows a dépassé un seuil prédéfini. Le manque d'espace disque peut entraîner des pénuries d'espace disque Ce sont des Direct-Customer-Alerts alarmes.
Amazon EFS	AMSEFSBurstCreditBalanceExhausted. BurstCreditBalance moins de 1000 pendant quinze minutes.	$ {EFS : :FileSystemId} : EFS : Solde créditeur éclatant CloudWatch alarme sur le système BurstCreditBalance de fichiers Amazon EFS.
Amazon EFS	AMSEFSClientConnectionsLimit. ClientConnections > 24 000 pendant quinze minutes.	$ {EFS : :FileSystemId} : EFS : limite de connexions client CloudWatch alarme sur le système ClientConnections de fichiers Amazon EFS.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
Amazon EFS	AMSEFSThroughputUtilization Limit. Utilisation du débit EFS > 80 % pendant une heure.	$ {EFS : :FileSystemId} : EFS : limite d'utilisation du débit CloudWatch alarme concernant l'utilisation du débit du système de fichiers Amazon EFS.
Amazon EFS	AMSEFSPercentIOLimit. Pourcentage IOLimit > 95 pendant soixante-quinze minutes.	$ {EFS : :FileSystemId} : EFS : pourcentage IOLimit CloudWatch alarme sur le pourcentage IOLimit du système de fichiers Amazon EFS.
Amazon EKS	Consultez Amazon EKSAlertes de base en matière de surveillance et de gestion des incidents pour Amazon EKS dans AMS Accelerate.	
Instance d'Elastic Load Balancing	SpilloverCountBack endConnectionErrors > 1 pendant 1 minute, 15 fois de suite.	LoadBalancer Alarme classique anti-débordement CloudWatch alarme si un nombre excessif de demandes ont été rejetées parce que la file d'attente est pleine.
Instance d'Elastic Load Balancing	HTTPCode_ELB_5xx_Count somme > 0 pendant 5 min, 3 fois de suite.	CloudWatch alarme en cas de nombre excessif de codes de réponse HTTP 5XX provenant de l'équilibreur de charge.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
Instance d'Elastic Load Balancing	SurgeQueueLength > 100 pendant 1 minute, 15 fois de suite.	Alarme LoadBalancer de longueur de file d'attente classique. CloudWatch alarme si un nombre excessif de demandes sont en attente de routage.
FSx pour ONTAP	AMSFSXONTAPIOPSUtilization. Utilisation des IOPS FSX:ONTAP > 80 % pendant deux heures.	$ {FSx: :FileSystemId} : Utilisation des IOPS par FSX:ONTAP CloudWatch alarme concernant la limite d'utilisation des IOPS de l'instance FSx for ONTAP.
FSx pour ONTAP	AMSFSXONTAPThroughputUtilisation. FSX : Utilisation du débit ONTAP > 80 % pendant deux heures.	$ {FSx: :FileSystemId} : Utilisation du débit de FSX:ONTAP CloudWatch alarme sur la limite de débit du volume FSx for ONTAP.
FSx pour ONTAP	AMSFSXONTAPVolumeInodeUtilization. Utilisation des inodes FSX:ONTAP > 80 % pendant deux heures.	$ {FSx: :FileSystemId} :$ {: :ONTAP FSx : :VolumeId } Utilisation de l'inode FSX:ONTAP CloudWatch alarme concernant la limite d'utilisation de la capacité de fichier du volume FSx for ONTAP.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
FSx pour ONTAP	AMSFSXONTAPVolumeCapacityUtilization. Utilisation de la capacité du volume FSX:ONTAP > 80 % pendant deux heures.	$ {FSx: :FileSystemId} :$ {: :ONTAP FSx : :} VolumeId CloudWatch alarme concernant la limite d'utilisation de la capacité du volume FSx pour ONTAP.
FSx pour le serveur de fichiers Windows	AMSFSXWindowsThroughputUtilization. FSX : utilisation du débit Windows > 80 % pendant deux heures.	$ {FSx: :FileSystemId} : FSX:Utilisation du débit Windows CloudWatch alarme concernant la limite de débit de l'instance FSx de serveur de fichiers Windows.
FSx pour le serveur de fichiers Windows	AMSFSXWindowsIOPSUtilization. FSX : utilisation des IOPS de Windows > 80 % pendant deux heures.	$ {FSx: :FileSystemId} : FSX : Utilisation des IOPS sous Windows CloudWatch alarme concernant la limite d'utilisation des IOPS de l'instance FSx de serveur de fichiers Windows.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
GuardDuty Service	Non applicable ; toutes les constatations (à des fins de menace) sont surveillées. Chaque résultat correspond à une alerte. Changements dans les GuardDuty résultats. Ces modifications incluent les nouveaux résultats obtenus et toutes les occurrences ultérieures de ces résultats existants.	Pour obtenir la liste des types de GuardDuty recherche pris en charge, consultez la section Types de recherche GuardDuty actifs.
Santé	AWS Health Dashboard	Des notifications sont envoyées lorsque le statut des événements AWS Health Dashboard (AWS Health) change en relation avec les services surveillés par AMS. Pour plus d'informations, consultez la section Services pris en charge.
IAM	Le profil d'instance Amazon EC2 IAM n'existe pas. Le profil d'instance IAM est manquant.	Pour obtenir des instructions sur le remplacement d'un profil d'instance Amazon EC2 IAM, consultez la documentation IAM sur Remplacer le rôle IAM.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
IAM	Le profil d'instance Amazon EC2 IAM comporte trop de politiques. Le profil d'instance IAM comporte 10 politiques et aucune politique supplémentaire ne peut être ajoutée.	• Modifiez le quota AWS de service pour IAM afin d'augmenter le nombre de politiques gérées par rôle à 20. Pour plus d'informations sur les quotas de service, consultez la section Affichage des quotas de service. • Réduisez le nombre de politiques gérées en dessous du quota IAM actuel en supprimant les politiques gérées inutiles pour le rôle IAM associé à ces instances. Assurez-vous de respecter les politiques requises par AMS. • Réduisez le nombre de politiques gérées en dessous du quota IAM actuel en consolidant les politiques pour le rôle IAM associé à ces instances. Assurez-vous de respecter les politiques requises par AMS. Pour les politiques requises par AMS, consultez le guide de l'utilisateur AMS Accelerate :Informations relatives à la

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
		modification des autorisations IAM.
Macie	Alertes nouvellement générées et mises à jour des alertes existantes. Macie trouve des changements dans les résultats. Ces modifications incluent les nouveaux résultats obtenus et toutes les occurrences ultérieures de ces résultats existants.	Alerte Amazon Macie. Pour obtenir la liste des types d'alertes Amazon Macie pris en charge, consultez la section Analyse des résultats d'Amazon Macie. Notez que Macie n'est pas activé pour tous les comptes.
NATGateways	PacketsDropCount : Alarme si le nombre de paquets est supérieur à 0 sur une période de 15 minutes	NatGateway PacketsDropCount Une valeur supérieure à zéro peut indiquer la présence d'un problème temporaire au niveau de la passerelle NAT.
NATGateways	ErrorPortAllocation : alarme si les passerelles NAT n'ont pas pu allouer de port pendant une période d'évaluation de plus de 15 minutes	NatGateway ErrorPortAllocation Nombre de fois où la passerelle NAT n'a pas pu allouer de port source. Une valeur supérieure à zéro indique que trop de connexions simultanées sont ouvertes.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
OpenSearch grappe	ClusterStatus le maximum rouge est >= 1 pendant 1 minute, 1 fois consécutive.	ClusterStatus rouge CloudWatch alarme. La clé de AWS KMS chiffrement utilisée pour chiffrer les données au repos dans votre domaine est désactivée. Réactivez-la pour revenir à un fonctionnement normal. Pour en savoir plus, consultez la section État du cluster rouge.
OpenSearch domaine	KMSKeyErreur >= 1 pendant 1 minute, 1 fois de suite.	Erreur de clé KMS CloudWatch alarme. Au moins une partition principale et ses réplicas ne sont pas alloués à un nœud. Pour en savoir plus, consultez la section Chiffrement des données au repos pour Amazon OpenSearch Service.
OpenSearch domaine	KMSKeyInaccessible >= 1 pendant 1 minute, 1 fois de suite.	Erreur d'inaccessibilité de la clé KMS CloudWatch alarme. Au moins une partition principale et ses réplicas ne sont pas alloués à un nœud. Pour en savoir plus, consultez la section Chiffrement des données au repos pour Amazon OpenSearch Service.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
OpenSearch domaine	ClusterStatus le maximum jaune est >= 1 pendant 1 minute, 1 fois consécutive.	ClusterStatus jaune Au moins une partition de réplica n'est pas allouée à un nœud. Pour en savoir plus, consultez la section État du cluster jaune.
OpenSearch domaine	FreeStorageSpace le minimum est <= 20480 pendant 1 minute, 1 fois consécutive.	Espace de stockage libre réduit Un nœud de votre cluster est descendu à 20 Gio d'espace de stockage disponible. Pour en savoir plus, consultez la section Manque d'espace de stockage disponible.
OpenSearch domaine	ClusterIndexWritesBlocked >= 1 pendant 5 minutes, 1 fois de suite.	Écritures bloquées dans l'index du cluster Le cluster bloque les demandes d'écriture. Pour en savoir plus, veuillez consulter la section ClusterBlockException.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
OpenSearch domaine	Nœuds minimum < x pendant 1 jour, 1 fois consécutive.	Nœuds en panne x est le nombre de nœuds de votre cluster. Cette alarme indique qu'au moins un nœud de votre cluster a été inaccessible pendant 1 jour. Pour en savoir plus, consultez la section Nœuds de cluster défaillants.
OpenSearch domaine	CPUUtilization moyenne >= 80 % pendant 15 minutes, 3 fois de suite.	Utilisation élevée du processeur dans le nœud de données 100 % d'utilisation de l'UC n'est pas rare, mais des moyennes élevées soutenues sont problématiques. Envisagez de dimensionner correctement un type d'instance existant ou d'ajouter des instances.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
OpenSearch domaine	JVMMemoryPression maximum >= 80 % pendant 5 minutes, 3 fois de suite.	Utilisation élevée de la mémoire dans le nœud de données Le cluster peut rencontre r des erreurs de mémoire insuffisante si l'utilisation augmente. Envisagez une mise à l'échelle verticale. OpenSearch utilise la moitié de la mémoire RAM d'une instance pour le tas Java, jusqu'à une taille de tas de 32 Gio. Vous pouvez mettre à l'échelle des instances verticalement jusqu'à 64 Gio de RAM, après quoi vous pouvez effectuer une mise à l'échelle horizontale en ajoutant des instances.
OpenSearch domaine	Maître CPUUtilization moyenne >= 50 % pendant 15 minutes, 3 fois de suite.	Utilisation élevée du processeur par Master Nodes Envisagez d'utiliser des types d'instances plus grands pour vos nœuds maîtres dédiés. En raison de leur rôle dans la stabilité du cluster et les déploiements bleu/vert, les nœuds principaux dédiés devraient avoir une utilisation d'UC moyenne inférieure à celle des nœuds de données.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
OpenSearch domaine	JVMMemoryPression principale maximum >= 80 % pendant 15 minutes, 1 fois de suite.	Pression de mémoire JVM élevée sur les nœuds principaux Envisagez d'utiliser des types d'instances plus grands pour vos nœuds maîtres dédiés. En raison de leur rôle dans la stabilité du cluster et les déploiements bleu/vert, les nœuds principaux dédiés devraient avoir une utilisation d'UC moyenne inférieure à celle des nœuds de données.
OpenSearch instance	AutomatedSnapshotFailure le maximum est >= 1 pendant 1 minute, 1 fois consécutive.	Défaillance du snapshot automatique CloudWatch alarme. Un instantané automatique a échoué. Cette défaillance est souvent le résultat d'un état de santé de cluster rouge. Pour en savoir plus, consultez la section État du cluster rouge.
Amazon RDS	Utilisation moyenne du processeur > 90 % pendant 15 minutes, 2 fois de suite.	$ {RDS : : DBInstance Identifiant} : CPUUtilization CloudWatch alarmes.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
Amazon RDS	Somme de DiskQueueDepth > 75 % pendant 1 minute, 15 fois de suite.	$ {RDS : : DBInstance Identifiant} : DiskQueue CloudWatch alarmes.
Amazon RDS	Moyenne FreeStorageSpace < 1 073 741 824 octets pendant 5 minutes, 2 fois de suite.	$ {RDS : : DBInstance Identifiant} : FreeStorageSpace CloudWatch alarmes.
Amazon RDS	Alerte de faible capacité de stockage Se déclenche lorsque le stockage alloué à l'instance de base de données est épuisé.	RDS-EVENT-0007, consultez la section Utilisation des notifications d'événements Amazon RDS.
Amazon RDS	L'instance de base de données échoue L'instance de base de données a échoué en raison d'une configuration incompatible ou d'un problème de stockage sous-jacent. Commencez un point-in-time-restore pour l'instance de base de données.	RDS-EVENT-0031, consultez les informations détaillées sur Catégories d'événements et messages d'événements Amazon RDS.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
Amazon RDS	Le basculement sur RDS -0034 n'a pas été tenté. Amazon RDS ne tente pas le basculement demandé, car un basculement s'est récemment produit sur l'instance de base de données.	RDS-EVENT-0034, consultez les informations détaillées sur Catégories d'événements et messages d'événements Amazon RDS.
Amazon RDS	RDS - Paramètres non valides de l'instance de base de données 0035 Par exemple, MySQL n'a pas pu démarrer car un paramètre lié à la mémoire est défini trop haut pour cette classe d'instance. Vous devez donc modifier le paramètre de mémoire et redémarrer l'instance de base de données.	RDS-EVENT-0035, consultez les informations détaillées sur Catégories d'événements et messages d'événements Amazon RDS.
Amazon RDS	Instance de IDs base de données de sous-réseau non valide L'instance de base de données se trouve sur un réseau non compatibl e. Certains sous-réseaux spécifiés ne IDs sont pas valides ou n'existent pas.	Événement de service. RDS-EVENT-0036, consultez les informations détaillées sur Catégories d'événements et messages d'événements Amazon RDS.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
Amazon RDS	Erreur de lecture de la réplique de l'instance de base de données RDS-0045 Une erreur s'est produite lors du processus de réplication en lecture. Pour plus d'informations, consultez le message de l'évènement. Pour plus d'informations sur la résolution des erreurs de lecture de répliques, consultez la section Résolution d'un problème de réplication de lecture MySQL.	RDS-EVENT-0045, consultez les informations détaillées sur Catégories d'événements et messages d'événements Amazon RDS.
Amazon RDS	RDS-0057 Erreur lors de la création du compte utilisateur statspack La réplication sur le Read Replica est terminée.	Événement de service. RDS-EVENT-0057, consultez les informations détaillées sur Catégories d'événements et messages d'événements Amazon RDS.
Amazon RDS	Fin de la réplication en lecture de l'instance de base de données RDS-0058 Erreur lors de la création du compte d'utilisateur Statspack PERFSTAT. Supprimez le compte avant d'ajouter l'option Statspack.	Événement de service. RDS-EVENT-0058, consultez les informations détaillées sur Catégories d'événements et messages d'événements Amazon RDS.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
Amazon RDS	Début de la restauration de l'instance de base L'instance de base de données SQL Server est en train de rétablir son miroir. Les performances seront dégradées tant que le miroir n'est pas restauré. Il a été trouvé une base de données avec un modèle de récupérat ion autre que FULL. Le modèle de restauration est redevenu FULL et la restaurat ion par mise en miroir a été lancée. (<dbname>: <recovery model found>[,...])	Événement de service. RDS-EVENT-0066 pour en savoir plus, consultez les catégories d'événements et les messages d'événements Amazon RDS.
Amazon RDS	Un basculement pour le cluster de base de données a échoué.	RDS-EVENT-0069, consultez les informations détaillées sur Catégories d'événements et messages d'événements Amazon RDS.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
Amazon RDS	Compartiment S3 de récupération d'autorisations non valides Le rôle IAM que vous utilisez pour accéder à votre compartiment Amazon S3 pour la sauvegarde et la restauration natives SQL Server est mal configuré. Pour plus d'informations, consultez Configuration de la sauvegarde et de la restauration natives.	Événement de service. RDS-EVENT-0081 pour en savoir plus, consultez les catégories d'événements et les messages d'événements Amazon RDS.
Amazon RDS	Aurora n'a pas pu copier les données de sauvegarde d'un compartiment Amazon S3.	RDS-EVENT-0082, consultez les informations détaillées sur Catégories d'événements et messages d'événements Amazon RDS.
Amazon RDS	Alerte de faible capacité de stockage lorsque l'instance de base de données a consommé plus de 90 % du stockage alloué.	Événement de service. RDS-EVENT-0089 pour en savoir plus, consultez les catégories d'événements et les messages d'événements Amazon RDS.
Amazon RDS	Service de notification en cas d'échec du dimensionnement pour le cluster de base de données Aurora Serverless.	Événement de service. RDS-EVENT-0143 pour en savoir plus, consultez les catégories d'événements et les messages d'événements Amazon RDS.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
Amazon RDS	L'instance de base de données est à un état non valide. Aucune action n'est nécessaire. La scalabilité automatique retentera plus tard.	RDS-EVENT-0219, consultez les informations détaillées sur les catégories d'événements et les messages d'événements Amazon RDS.
Amazon RDS	L'instance de base de données a atteint le seuil de stockage complet et la base de données a été arrêtée.	RDS-EVENT-0221, consultez les informations détaillées sur les catégories d'événements et les messages d'événements Amazon RDS.
Amazon RDS	Cet événement indique que le dimensionnement automatiq ue du stockage de l'instanc e Amazon RDS n'est pas en mesure de s'adapter. Plusieurs raisons peuvent expliquer l'échec du dimension nement automatique.	RDS-EVENT-0223, consultez les informations détaillées sur Catégories d'événements et messages d'événements Amazon RDS.
Amazon RDS	La scalabilité automatique du stockage a déclenché une tâche de mise l'échelle du stockage en attente qui atteindrait le seuil de stockage maximal.	RDS-EVENT-0224, consultez les informations détaillées sur Catégories d'événements et messages d'événements Amazon RDS.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
Amazon RDS	L'instance de base de données comporte un type de stockage qui est actuellement indisponible dans la zone de disponibilité. La scalabilité automatique retentera plus tard.	RDS-EVENT-0237, consultez les informations détaillées sur Catégories d'événements et messages d'événements Amazon RDS.
Amazon RDS	Amazon RDS n'a pas pu fournir de capacité pour le proxy car il n'y a pas suffisamment d'adresses IP disponibles dans vos sous-réseaux.	RDS-EVENT-0243, consultez les informations détaillées sur Catégories d'événements et messages d'événements Amazon RDS.
Amazon RDS	Votre espace de stockage Compte AWS a dépassé le quota de stockage autorisé.	RDS-EVENT-0254, consultez les informations détaillées sur Catégories d'événements et messages d'événements Amazon RDS.
Cluster Amazon Redshift	L'état du cluster lorsqu'il n'est pas en mode maintenance < 1 pendant 5 minutes	RedshiftClusterHealthStatus Pour plus d'informations, consultez la section Surveillance d'Amazon Redshift à l'aide CloudWatch de métriques.

Type de service/ressource	Source de l'alerte et état du déclencheur	Nom et notes de l'alerte
Site-to-Site VPN	VPNTunnelVers le bas TunnelState <= 0 pendant 1 min, 20 fois de suite.	$ {AWS::EC2::VpnConnectionId} - En VPNTunnel panne TunnelState est 0 lorsque les deux tunnels sont en panne, 0,5 lorsqu'un tunnel est en haut et 1,0 lorsque les deux tunnels sont en haut.
Agent Systems Manager	EC2 Instances non gérées par Systems Manager L'agent SSM n'est pas installé. L'agent SSM est installé sur l'instance, mais le service d'agent n'est pas en cours d'exécution. L'agent SSM n'a aucune route réseau vers le service AWS Systems Manager.	D'autres conditions peuvent perturber l'agent Systems Manager ; pour plus d'informations, consultez la section Résolution des problèmes de disponibilité des nœuds gérés.

Pour plus d'informations sur les mesures correctives, voirCorrection automatique des alertes par AMS.

Regardez la vidéo d'Andrew pour en savoir plus (7:03)

Notifications d'incidents liées aux applications dans AMS

Utilisez les notifications d'incidents automatisées adaptées aux applications pour personnaliser votre expérience de communication pour les demandes d'assistance créées par AMS en votre nom. Lorsque vous utilisez cette fonctionnalité, AMS extrait les préférences de charge de travail personnalisées AWS Service Catalog AppRegistryafin d'enrichir vos communications relatives aux incidents AMS avec des métadonnées relatives à vos applications et de personnaliser la gravité des

demandes d'assistance créées par AMS en votre nom. Pour utiliser cette fonctionnalité, vous devez d'abord intégrer AWS Service Catalog AppRegistry.

Pour en savoir plus sur les paramètres de surveillance par défaut d'AMS Accelerate, consultezSurveillance et gestion des événements dans AMS Accelerate.

Intégrez AppRegistry et créez des applications

Pour intégrer AppRegistry, consultez la section Getting started with AppRegistry dans le guide de AWS Service Catalog AppRegistry l'administrateur. Après l'intégration, utilisez l'une des méthodes suivantes pour créer des applications :

1. AWS console : pour en savoir plus sur la création d'une application AppRegistry via la AWS console, consultez la section Création d'applications dans le guide de l'AWS Service Catalog AppRegistry administrateur.
2. CloudFormation: Vous pouvez définir votre AppRegistry application comme n'importe quelle autre ressource. Pour plus d'informations, consultez Référence du type de ressource AWS Service Catalog AppRegistry dans le Guide de l'utilisateur AWS CloudFormation .
3. Automatisation AMS : Pour simplifier le processus d'enregistrement des applications, AMS vous fournit le document `AWSManagedServices-CreateAppRegistryApplication` d'automatisation SSM. Pour utiliser cette méthode, appelez le document depuis la AWS Systems Manager console à https://console.aws.amazon.com/systems-manager/, ou avec le, AWS CLI comme décrit dans l'exemple suivant.

```
# The following registers a new application with customized severity
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["normal"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# The following registers a new application with no customizations
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
```

```
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# You can also register applications using CloudFormation stacks
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["STACKS"],"AppTagValue":
[""],"CFNStackNames":["arn:aws:cloudformation:us-east-1:123456789012:stack/
stack-2343eddq/1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p"],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
```

Créez des balises pour permettre l'enrichissement des dossiers

Vous devez étiqueter vos applications pour qu'AMS puisse accéder aux métadonnées des applications. Le tableau suivant répertorie les balises requises.

Les balises avec le préfixe `ams:rt:` sont appliquées via Resource Tagger.

Clé de balise	Valeur de balise
géré par des tiers	true
ams:rt:ams-managed	true

Personnalisez la gravité des demandes de support AMS en fonction de vos applications

Vous pouvez personnaliser la gravité des demandes de support créées par AMS en spécifiant le degré d'importance de votre application pour votre organisation. Ce paramètre est contrôlé par un groupe d'attributs associé à votre application dans AppRegistry. Le nom du groupe d'attributs doit correspondre au modèle suivant :

```
AMS.<ApplicationName>.CommunicationOptions
```

Dans le modèle précédent, le nom `ApplicationName` doit correspondre au nom utilisé AppRegistry lors de la création de l'application.

Exemple de contenu :

```
{
"SchemaVersion": "1.0",
"Criticality": "low"
}
```

SchemaVersion

Cela détermine la version du schéma que vous utilisez et le sous-ensemble de fonctionnalités disponibles.

Version du schéma	Fonctionnalité
1.0	Gravité personnalisée des demandes d'assistance en fonction de la valeur de criticité

Criticité

La criticité de cette application détermine la gravité des demandes de support créées par les systèmes automatisés AMS.

Valeurs valides :

```
low|normal|high|urgent|critical
```

Pour plus d'informations sur les niveaux de gravité, consultez SeverityLevella référence de l'AWS Support API.

Obligatoire : oui

Vérifiez les autorisations requises

Pour utiliser cette fonctionnalité, AMS doit avoir accès aux AWS Identity and Access Management autorisations suivantes :

- iam : ListRoleTags

- iam : ListUserTags
- API de balisage des groupes de ressources : GetResources
- servicecatalog-appregistry : GetApplication
- servicecatalog-appregistry : ListAssociatedAttributeGroups
- servicecatalog-appregistry : GetAttributeGroup

> **Important**
>
> Assurez-vous qu'aucune politique IAM ou politique de contrôle des services (SCP) ne refuse les actions précédentes.

Les appels d'API sont effectués par le `ams-access-admin` rôle. Voici un exemple de ce que vous pourriez voir :

```
arn:aws:sts::111122223333:assumed-role/ams-access-admin/AMS-AMSAppMetadataLookup-*
```

Accélérer Alarm Manager

AMS Accelerate applique des alarmes à vos AWS ressources à l'aide du gestionnaire d'alarmes basé sur des balises pour mettre en œuvre une stratégie de surveillance de base et garantir que toutes vos AWS ressources sont surveillées et protégées. En intégrant le gestionnaire d'alarme basé sur des balises, vous pouvez personnaliser la configuration de vos AWS ressources en fonction de leur type, de leur plate-forme et d'autres balises, afin de garantir la surveillance des ressources. Alarm Manager est déployé sur votre compte Accelerate lors de l'intégration.

Comment fonctionne Alarm Manager

Lorsque votre compte est intégré à AMS Accelerate, deux documents JSON, appelés profils de configuration, sont déployés dans votre compte dans. AWS AppConfig Les deux documents de profil se trouvent dans l'application Alarm Manager et dans l'environnement d'infrastructure AMS Accelerate.

Les deux profils de configuration sont nommés AMSManagedAlarms (profil de configuration par défaut) et CustomerManagedAlarms(profil de configuration de personnalisation).

- Profil de configuration par défaut :

  - La configuration trouvée dans ce profil contient la configuration par défaut déployée par AMS Accelerate dans tous les comptes clients. Cette configuration contient la politique de surveillance AMS Accelerate par défaut, que vous ne devez pas modifier car AMS Accelerate peut mettre à jour ce profil à tout moment, en effaçant toutes les modifications que vous avez apportées.
  - Si vous souhaitez modifier ou désactiver l'une de ces définitions, reportez-vous aux sections Modification de la configuration par défaut de l'alarme Accelerate etDésactivation de la configuration d'alarme Accelerate par défaut.
- Profil de configuration de personnalisation :
  - Toute configuration de ce profil est entièrement gérée par vous ; AMS Accelerate ne remplace pas ce profil, sauf si vous le demandez explicitement.
  - Vous pouvez spécifier toutes les définitions d'alarme personnalisées que vous souhaitez dans ce profil, et vous pouvez également spécifier des modifications à apporter à la configuration par défaut gérée par AMS Accelerate. Pour plus d'informations, consultez Modification de la configuration par défaut de l'alarme Accelerate et Désactivation de la configuration d'alarme Accelerate par défaut.
  - Si vous mettez à jour ce profil, Alarm Manager applique automatiquement vos modifications à toutes les ressources pertinentes de votre AWS compte. Notez que même si vos modifications sont appliquées automatiquement, elles peuvent prendre jusqu'à 60 minutes pour prendre effet.
  - Vous pouvez mettre à jour ce profil à l'aide des CLI/SDK outils AWS Management Console ou AWS. Consultez le guide de AWS AppConfig l'utilisateur pour obtenir des instructions sur la mise à jour d'une configuration.
  - Le profil de personnalisation est initialement vide ; toutefois, toutes les définitions d'alarme placées dans le document de profil sont appliquées, en plus de la configuration par défaut.

Toutes les CloudWatch alarmes créées par le gestionnaire d'alarmes contiennent le tag key ams:alarm-manager:managed et la valeur du tag true. Cela permet de garantir que le gestionnaire d'alarmes ne gère que les alarmes qu'il crée et qu'il n'interfère avec aucune de vos propres alarmes. Vous pouvez voir ces balises à l'aide de l' CloudWatch ListTagsForResourceAPI Amazon.

> **Important**
>
> Si les définitions d'alarme personnalisées et les définitions d'alarme par défaut sont spécifiées avec le même identifiant de configuration (voirAccélérer le profil de configuration : surveillance), les définitions personnalisées ont la priorité sur les règles par défaut.

Commencer à utiliser Accelerate Alarm Manager

Par défaut, lorsque vous intégrez AMS Accelerate, votre configuration est déployée pour AWS AppConfig définir une base d'alarme pour vos ressources. Les définitions d'alarme ne sont appliquées qu'aux ressources dotées des balises ams:rt : *. Nous recommandons d'appliquer ces balises à l'aide de Accélérez Resource Tagger : vous configurez une configuration de base de Resource Tagger afin de faire savoir à AMS Accelerate quelles ressources vous souhaitez gérer.

Utilisez Resource Tagger pour appliquer la clé de balise ams:rt:ams-managed avec une valeur de balise true à toutes les ressources que vous souhaitez qu'AMS Accelerate surveille.

Voici un exemple de profil de personnalisation de Resource Tagger que vous pouvez utiliser pour activer la surveillance de toutes vos EC2 instances Amazon. Pour obtenir des informations générales, consultez Accélérez Resource Tagger.

```
{
    "AWS::EC2::Instance": {
        "AMSManageAllEC2Instances": {
            "Enabled": true,
            "Filter": {
                "InstanceId": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

Pour plus d'informations sur la façon d'appliquer cette configuration de Resource Tagger, consultezAfficher ou modifier la configuration du Resource Tagger.

Accelerate Alarm Manager tags

Par défaut, lorsque vous intégrez AMS Accelerate, votre configuration est déployée pour AWS AppConfig définir une base d'alarme pour vos ressources. Les définitions d'alarme sont appliquées uniquement aux ressources dotées des balises ams:rt : *. Nous recommandons d'appliquer ces

balises à l'aide de Accélérez Resource Tagger : vous configurez une configuration de base de Resource Tagger afin de faire savoir à AMS Accelerate quelles ressources vous souhaitez gérer.

Utilisez Resource Tagger pour appliquer la clé de balise ams:rt:ams-managed avec une valeur de balise true à toutes les ressources que vous souhaitez qu'AMS Accelerate surveille.

Rubriques

- Accélérez les balises à l'aide de Resource Tagger
- Accélérez les tags sans Resource Tagger
- Accélérez les tags en utilisant AWS CloudFormation
- Accélérez les tags à l'aide de Terraform

Accélérez les balises à l'aide de Resource Tagger

Le gestionnaire d'alarmes basé sur des balises gère le cycle de vie des CloudWatch alarmes par ressource ; toutefois, il exige que les ressources gérées possèdent des balises spécifiques définies par AMS Accelerate. Pour utiliser le Resource Tagger afin d'appliquer l'ensemble par défaut d'alarmes gérées par AMS aux instances basées sur Linux et Windows, procédez comme suit.

1. Accédez à la AppConfigconsole depuis votre compte.
2. Sélectionnez l' ResourceTagger application.
3. Sélectionnez l'onglet Profils de configuration, puis sélectionnez CustomerManagedTags.
4. Cliquez sur Créer pour créer un nouveau profil.
5. Sélectionnez JSON et définissez votre configuration. Pour plus d'exemples de définition de filtres et de plateformes, consultezAccélérez Resource Tagger.

```
{
"AWS::EC2::Instance": {
   "MonitorAllInstances": {
       "Enabled": true,
       "Filter": {
           "Platform": "*"
       },
       "Tags": [
           {
               "Key": "ams:rt:ams-managed",
               "Value": "true"
           }
```

```
        ]
    }
}
}
```

6. Cliquez sur Créer une version de configuration hébergée.
7. Cliquez sur Démarrer le déploiement.
8. Définissez les détails de déploiement suivants :

```
Environment: AMSInfrastructure Hosted configuration version: <Select the version
 that you have just created>
              Deployment Strategy: AMSNoBakeDeployment
```

9. Cliquez sur Démarrer le déploiement.

Vos instances sont étiquetées`"ams:rt:ams-managed": "true"`, ce qui garantit que `"ams:rt:ams-monitoring-policy": "ams-monitored"` des `"ams:rt:ams-monitoring-policy-platform": "ams-monitored-linux"` informations supplémentaires sont appliquées aux instances. Ces balises entraînent ensuite la création des alarmes appropriées pour l'instance. Pour plus d'informations sur ce processus, consultez Surveillance dans Accelerate.

Regardez la vidéo de Himanshu pour en savoir plus (11:04)

Accélérez les tags sans Resource Tagger

Le gestionnaire d'alarmes basé sur des balises gère le cycle de vie des CloudWatch alarmes par ressource ; toutefois, il exige que les ressources gérées possèdent des balises spécifiques définies par AMS Accelerate. AMS Accelerate fournit un profil de configuration par défaut qui suppose que vos balises ont été appliquées par Resource Tagger.

Si vous souhaitez utiliser une autre méthode pour appliquer des balises à vos ressources, telle que AWS CloudFormation Terraform, et non le Resource Tagger, vous devez désactiver le Resource Tagger afin qu'il n'applique pas de balises à vos ressources et qu'il n'entre pas en concurrence avec la méthode de balisage que vous avez choisie. Pour obtenir des instructions sur la modification de votre profil de configuration personnalisé de Resource Tagger afin d'activer le mode lecture seule, consultez. Empêcher le Resource Tagger de modifier les ressources

Une fois que le baliseur de ressources a été configuré en mode lecture seule et que le profil de configuration a été déployé, utilisez la méthode de balisage que vous avez choisie pour appliquer des balises à vos ressources conformément aux directives suivantes :

Type de ressource	Clé de balise	Valeur de balise
Toutes les ressources prises en charge (décrites dans ce tableau)	ams : rt : ams-monitoring-policy	surveillée par AMS
EC2 instances (Linux)	ams : rt : ams-monitoring-policy-platform	ams-monitored-linux
EC2 instances (Windows)	ams : rt : ams-monitoring-policy-platform	ams-monitored-windows
OpenSearch Domaine avec KMS	ams : rt : ams-monitoring-with-kms	ams-monitored-with-kms
OpenSearch Domaine avec nœud principal dédié	ams : rt : ams-monitoring-with-master	ams-monitored-with-master

Les ressources dotées de ces clés et valeurs de balise sont gérées par le gestionnaire d'alarme AMS Accelerate.

Accélérez les tags en utilisant AWS CloudFormation

> **Note**
>
> Assurez-vous d'avoir configuré Resource Tagger en mode lecture seule avant d'appliquer des balises AWS CloudFormation, sinon Resource Tagger peut modifier les balises en fonction du profil de configuration. Pour plus d'informations sur le réglage du Resource Tagger en mode lecture seule et pour savoir comment fournir vos propres balises, consultez. Accélérez les tags sans Resource Tagger

Pour appliquer des balises AWS CloudFormation, vous pouvez appliquer des balises au niveau de la pile (voir Balises de CloudFormation ressources) ou au niveau de chaque ressource (par exemple, voir Création de balises d' EC2 instance).

Voici un exemple de la façon dont vous pouvez appliquer les balises de gestion des alarmes AMS Accelerate à une EC2 instance Amazon gérée par AWS CloudFormation :

```
Type: AWS::EC2::Instance
Properties:
 InstanceType: "t3.micro"

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

Voici un exemple de la façon dont vous pouvez appliquer les balises de gestion des alarmes AMS Accelerate à un groupe Auto Scaling géré par AWS CloudFormation. Notez que le groupe Auto Scaling propagera ses balises aux EC2 instances Amazon qu'il a créées :

```
Type: AWS::AutoScaling::AutoScalingGroup
Properties:
 AutoScalingGroupName: "TestASG"

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

Accélérez les tags à l'aide de Terraform

> **Note**
>
> Assurez-vous d'avoir configuré Resource Tagger en mode lecture seule avant d'appliquer des balises AWS CloudFormation, sinon Resource Tagger peut modifier les balises en fonction du profil de configuration. Pour plus d'informations sur le réglage du Resource Tagger en mode lecture seule et pour savoir comment fournir vos propres balises, consultez. Accélérez les tags sans Resource Tagger

Pour une description de la gestion des balises de ressources à l'aide de Terraform, consultez la documentation Terraform Resource Tagging.

Voici un exemple de la manière dont vous pouvez appliquer les balises de gestion des alarmes AMS Accelerate à une EC2 instance Amazon gérée par Terraform.

```
resource "aws_instance" "test_linux_instance" {
     # ...ami and other properties...

     instance_type = "t3.micro"

     tags = {
       "aws:rt:ams-monitoring-policy" = "ams-monitored"
       "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
     }
   }
```

Voici un exemple de la manière dont vous pouvez appliquer des balises de gestion des alarmes AMS à un groupe Auto Scaling géré par Terraform. Notez que le groupe Auto Scaling propage ses balises aux EC2 instances qu'il a créées :

```
 resource "aws_autoscaling_group" "test_asg" {
 name = "terraform-test"
 # ...other properties...

 tags = {
   "aws:rt:ams-monitoring-policy" = "ams-monitored"
   "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
 }
}
```

Accélérer les profils de configuration du gestionnaire d'alarme

Lorsque votre compte est intégré à AMS Accelerate, deux documents JSON, appelés profils de configuration, sont déployés dans votre compte avec AWS AppConfig (voir Qu'est-ce que c'est AWS AppConfig). Les deux documents de profil se trouvent dans l'application Alarm Manager et dans l'environnement d'infrastructure AMS Accelerate.

Rubriques

- Accélérer le profil de configuration : surveillance
- Accélérer le profil de configuration : substitution de pseudoparamètres
- Exemples de configuration d'alarmes accélérés
- Affichage de la configuration de votre Accelerate Alarm Manager
- Modification de la configuration de l'alarme Accelerate
- Modification de la configuration par défaut de l'alarme Accelerate
- Déploiement Accélérez les modifications de configuration des
- Annulation accélérée des changements d'alarme
- Conserver les alarmes Accel
- Désactivation de la configuration d'alarme Accelerate par défaut

Accélérer le profil de configuration : surveillance

Le document de profil de configuration par défaut et le document de profil de configuration de personnalisation suivent la même structure :

```
  {
    "<ResourceType>": {
        "<ConfigurationID>": {
            "Enabled": true,

            "Tag": {
                "Key": "...",
                "Value": "..."
            },
            "AlarmDefinition": {
                ...
            }
        },
        "<ConfigurationID>": {
            ...
        }
    },
    "<ResourceType>": {
        ...
    }
}
```

- ResourceType: Cette clé doit être l'une des chaînes prises en charge suivantes. La configuration au sein de cet objet JSON ne portera que sur le type de AWS ressource spécifié. Types de ressource pris en charge :

```
AWS::EC2::Instance
AWS::EC2::Instance::Disk
AWS::RDS::DBInstance
AWS::RDS::DBCluster
AWS::Elasticsearch::Domain
AWS::OpenSearch::Domain
AWS::Redshift::Cluster
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::ElasticLoadBalancingV2::LoadBalancer::TargetGroup
AWS::ElasticLoadBalancing::LoadBalancer
AWS::FSx::FileSystem::ONTAP
AWS::FSx::FileSystem::ONTAP::Volume
AWS::FSx::FileSystem::Windows
AWS::EFS::FileSystem
AWS::EC2::NatGateway
AWS::EC2::VPNConnection
```

- ConfigurationID : cette clé doit être unique dans le profil et nommer de manière unique le bloc de configuration suivant. Si deux blocs de configuration d'un même ResourceTypebloc ont le même identifiant de configuration, celui qui apparaît le plus récent dans le profil prend effet. Si vous spécifiez dans votre profil de personnalisation un identifiant de configuration identique à celui spécifié dans le profil par défaut, le bloc de configuration défini dans le profil de personnalisation prend effet.
  - Activé : (facultatif, default=true) Spécifiez si le bloc de configuration prendra effet. Définissez ce paramètre sur false pour désactiver un bloc de configuration. Un bloc de configuration désactivé se comporte comme s'il n'était pas présent dans le profil.
  - Tag : Spécifiez le tag auquel s'applique cette définition d'alarme. Toute ressource (du type de ressource approprié) qui possède cette clé et cette valeur de balise aura une CloudWatch alarme créée avec la définition donnée. Ce champ est un objet JSON avec les champs suivants :
    - Clé : clé de la balise à associer. N'oubliez pas que si vous utilisez Resource Tagger pour appliquer les balises à la ressource, la clé de la balise commencera toujours par ams:rt :.
    - Valeur : valeur de la balise à mettre en correspondance.
  - AlarmDefinition: Définit l'alarme à créer. Il s'agit d'un objet JSON dont les champs sont transmis tels quels à l'appel d' CloudWatch `PutMetricAlarm`API (à l'exception des

pseudoparamètres ; pour plus d'informations, voirAccélérer le profil de configuration : substitution de pseudoparamètres). Pour plus d'informations sur les champs obligatoires, consultez la PutMetricAlarmdocumentation.

OU

CompositeAlarmDefinition: Définit une alarme composite à créer. Lorsque vous créez une alarme composite, vous spécifiez une expression de règle pour l'alarme qui prend en compte l'état des autres alarmes que vous avez créées. Il s'agit d'un objet JSON dont les champs sont transmis tels quels au`CloudWatchPutCompositeAlarm`. L'alerte composite passe à l'état ALARM uniquement si toutes les conditions de la règle sont remplies. Les alertes spécifiées dans l'expression de règle d'alerte composite peuvent inclure des alertes de métrique et d'autres alertes composites. Pour plus d'informations sur les champs obligatoires, consultez la PutCompositeAlarmdocumentation.

Les deux options fournissent les champs suivants :

- AlarmName: Spécifiez le nom de l'alarme que vous souhaitez créer pour la ressource. Ce champ comporte les mêmes règles que celles spécifiées dans la PutMetricAlarmdocumentation ; toutefois, comme le nom de l'alarme doit être unique dans une région, le gestionnaire d'alarmes a une exigence supplémentaire : vous devez spécifier le pseudoparamètre de l'identifiant unique dans le nom de l'alarme (sinon, Alarm Manager ajoute l'identifiant unique de la ressource au début du nom de l'alarme). Par exemple, pour le type de AWS::EC2::Instanceressource, vous devez le spécifier `${EC2::InstanceId}` dans le nom de l'alarme, sinon il est implicitement ajouté au début du nom de l'alarme. Pour la liste des identifiants, voirAccélérer le profil de configuration : substitution de pseudoparamètres.

  Tous les autres champs sont tels que spécifiés dans la PutMetricAlarmPutCompositeAlarmdocumentation.
- AlarmRule: Spécifiez les autres alarmes à évaluer pour déterminer l'état de cette alarme composite. Pour chaque alarme à laquelle vous faites référence, elle doit exister CloudWatch ou être spécifiée dans le profil de configuration d'Alarm Manager de votre compte.

> **Important**
>
> Vous pouvez spécifier l'un AlarmDefinitionou l'autre ou CompositeAlarmDefinitiondans votre document de configuration d'Alarm Manager, mais les deux ne peuvent pas être utilisés en même temps.

Dans l'exemple suivant, le système crée une alarme lorsque deux alarmes métriques spécifiées dépassent son seuil :

```
{
  "AWS::EC2::Instance": {
    "LinuxResourceAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:mylinuxinstance",
        "Value": "true"
      },
      "CompositeAlarmDefinition": {
        "AlarmName": "${EC2::InstanceId} Resource Usage High",
        "AlarmDescription": "Alarm when a linux EC2 instance is using too much CPU and
 too much Disk",
        "AlarmRule": "ALARM(\"${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}\") AND ALARM(\"${EC2::InstanceId}: CPU Too High\")"
      }
    }
  }
}
```

> **Important**
>
> Lorsque Alarm Manager n'est pas en mesure de créer ou de supprimer une alarme en raison d'une configuration défectueuse, il envoie la notification à la rubrique Direct-Customer-Alerts SNS. Cette alarme est appelée AlarmDependencyError.
>
> Nous vous recommandons vivement de confirmer votre inscription à cette rubrique SNS. Pour recevoir des messages publiés dans un sujet, vous devez abonner un point de terminaison au sujet. Pour plus de détails, voir Étape 1 : Création d'un sujet.

> **Note**
>
> Lorsque des alarmes de détection d'anomalies sont créées, Alarm Manager crée automatiquement les modèles de détection d'anomalies requis pour les métriques spécifiées. Lorsque les alarmes de détection d'anomalies sont supprimées, Alarm Manager ne supprime pas les modèles de détection d'anomalies associés.
> Amazon CloudWatch limite le nombre de modèles de détection d'anomalies que vous pouvez avoir dans une AWS région donnée. Si vous dépassez le quota du modèle, Alarm Manager ne crée pas de nouvelles alarmes de détection d'anomalies. Vous devez soit supprimer les modèles non utilisés, soit contacter votre partenaire AMS pour demander une augmentation de limite.
> La plupart des définitions d'alarme de base fournies par AMS Accelerate citent le sujet SNS, MS-Topic, comme cible. Il est destiné à être utilisé dans le service de surveillance AMS Accelerate et constitue le mécanisme de transport pour que vos notifications d'alarme soient transmises à AMS Accelerate. Ne spécifiez pas MMS-Topic comme cible pour les alarmes autres que celles fournies dans la ligne de base (et les remplacements de celles-ci), car le service ignore les alarmes inconnues. Cela n'entraîne pas l'action d'AMS Accelerate sur vos alarmes personnalisées.

Accélérer le profil de configuration : substitution de pseudoparamètres

Dans l'un ou l'autre des profils de configuration, vous pouvez spécifier des pseudoparamètres qui sont substitués sur place comme suit :

- Global, n'importe où dans le profil :
  - $ {AWS::AccountId} : remplacé par votre identifiant de AWS compte
  - $ {AWS::Partition} : Remplacé par la partition dans laquelle se trouve Région AWS la ressource (il s'agit de « aws » pour la plupart des régions) ; pour plus d'informations, consultez l'entrée relative à la partition dans la référence ARN.
  - $ {AWS::Region} : remplacé par le nom de la région dans laquelle votre ressource est déployée (par exemple us-east-1)
- Dans un bloc AWS::EC2::Instancede type de ressource :
  - $ {EC2: :InstanceId} : (identifiant) remplacé par l'ID d'instance de votre EC2 instance Amazon.
  - $ {EC2: :InstanceName} : remplacé par le nom de votre EC2 instance Amazon.
- Dans un bloc de type de ressource AWS::EC2::Instance::Disk :

  - $ {EC2: :InstanceId} : (identifiant) Remplacé par l'ID d'instance de votre EC2 instance Amazon.
  - $ {EC2: :InstanceName} : Remplacé par le nom de votre EC2 instance Amazon.
  - $ {EC2: :Disk : :Device} : (identifiant) Remplacé par le nom du disque. (Linux uniquement, sur les instances gérées par l'CloudWatch agent).
  - $ {EC2: :Disk : :FSType} : (identifiant) Remplacé par le type de système de fichiers du disque. (Linux uniquement, sur les instances gérées par le CloudWatchAgent).
  - $ {EC2: :Disk : :Path} : (identifiant) Remplacé par le chemin du disque. Sous Linux, il s'agit du point de montage du disque (par exemple,/), tandis que sous Windows, il s'agit de l'étiquette du lecteur (par exemple, c :/) (uniquement sur une instance gérée par l'CloudWatch agent).
  - $ {EC2: :Disk : :UUID} : (identifiant) Remplacé par un UUID généré qui identifie le disque de manière unique, celui-ci doit être spécifié dans le nom de l'alarme, car une alarme de type AWS::EC2::Instance::Disk ressource créera une alarme par volume. La spécification de $ {EC2: :Disk : :UUID} préservera l'unicité des noms d'alarme.
- Dans un bloc AWS::EKS::Clusterde type de ressource :
  - $ {EKS : :ClusterName} : (identifiant) remplacé par le nom de votre cluster EKS.
- Dans un bloc AWS::OpenSearch::Domainde type de ressource :
  - $ {OpenSearch: :DomainName} : (identifiant) remplacé par le nom de votre domaine EKS.
- Dans un bloc AWS::ElasticLoadBalancing::LoadBalancerde type de ressource :
  - $ {ElasticLoadBalancing: LoadBalancer : :Name} : (identifiant) remplacé par le nom de votre V1 Load Balancer.
- Dans un bloc AWS::ElasticLoadBalancingV2::LoadBalancerde type de ressource :
  - $ {ElasticLoadBalancingV2 : LoadBalancer : :Arn} : (identifiant) remplacé par l'ARN de votre V2 Load Balancer.
  - $ {ElasticLoadBalancingV2 : LoadBalancer : :Name} : (identifiant) remplacé par le nom de votre V2 Load Balancer.
  - $ {ElasticLoadBalancingV2 : : LoadBalancer :FullName} : (identifiant) remplacé par le nom complet de votre V2 Load Balancer.
- Dans un bloc de type de TargetGroup ressource AWS::ElasticLoadBalancingV2::LoadBalancer: :
  - $ {ElasticLoadBalancingV2 : : TargetGroup :FullName} : (identifiant) remplacé par le nom du groupe cible de votre V2 Load Balancer.
  - $ {ElasticLoadBalancingV2 : TargetGroup : :UUID} : (identifiant) remplacé par un UUID généré pour votre V2 Load Balancer.

- Dans un bloc AWS::EC2::NatGatewayde type de ressource :
  - $ {NatGateway: :NatGatewayId} : (identifiant) remplacé par l'ID de passerelle NAT.
- Dans un bloc de type de DBInstance ressource AWS : :RDS : :
  - $ {RDS : : DBInstance Identifier} : (identifiant) remplacé par l'identifiant de votre instance de base de données RDS.
- Dans un bloc de type de DBCluster ressource AWS : :RDS : :
  - $ {RDS : : DBCluster Identifier} : (identifiant) remplacé par l'identifiant de votre cluster de base de données RDS.
- Dans un bloc AWS::Redshift::Clusterde type de ressource :
  - $ {Redshift : :ClusterIdentifier} : (identifiant) remplacé par l'identifiant de votre cluster Redshift.
- Dans un bloc AWS::Synthetics::Canaryde type de ressource :
  - $ {Synthetics : :} CanaryName : (identifiant) remplacé par le nom de votre CloudWatch canari Synthetics.
- Dans un bloc de type de VPNConnection ressource AWS EC2 : : : :
  - $ {AWS::EC2::VpnConnectionId} : (identifiant) remplacé par votre identifiant VPN.
- Dans un bloc AWS::EFS::FileSystemde type de ressource :
  - $ {EFS : :FileSystemId} : (identifiant) Remplacé par l'ID du système de fichiers de votre système de fichiers EFS.
- Dans un bloc de type de ressource AWS::FSx::FileSystem: :ONTAP :
  - $ {FSx: :FileSystemId} : (identifiant) Remplacé par l'ID du système de fichiers de votre système de fichiers FSX.
  - $ {FSx: FileSystem : :Throughput} : remplacé par le débit de votre système de fichiers FSX.
  - $ {FSx: FileSystem : :Iops} : remplacé par les IOPS du système de fichiers FSX.
- Dans un bloc de type de ressource AWS::FSx::FileSystem: :ONTAP : :Volume :
  - $ {FSx: :FileSystemId} : (identifiant) Remplacé par l'ID du système de fichiers de votre système de fichiers FSX.
  - $ {FSx: :ONTAP : :VolumeId} : (identifiant) Remplacé par l'ID du volume.
- Dans un bloc de type de ressource AWS::FSx::FileSystem::Windows :
  - $ {FSx: :FileSystemId} : (identifiant) Remplacé par l'ID du système de fichiers de votre système de fichiers FSX.
  - $ {FSx: FileSystem : :Throughput} : remplacé par le débit de votre système de fichiers FSX.

> **Note**
>
> Tous les paramètres marqués d'un identifiant sont utilisés comme préfixe pour le nom des alarmes créées, sauf si vous spécifiez cet identifiant dans le nom de l'alarme.

Exemples de configuration d'alarmes accélérés

Dans l'exemple suivant, le système crée une alarme pour chaque disque connecté à l'instance Linux correspondante.

```
{
    "AWS::EC2::Instance::Disk": {
        "LinuxDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mylinuxinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "disk_used_percent",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "device",
                        "Value": "${EC2::Disk::Device}"
                    },
                    {
                        "Name": "fstype",
                        "Value": "${EC2::Disk::FSType}"
                    },
                    {
                        "Name": "path",
                        "Value": "${EC2::Disk::Path}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
```

```
            }
        }
    }
}
```

Dans l'exemple suivant, le système crée une alarme pour chaque disque connecté à l'instance Windows correspondante.

```
{
     "AWS::EC2::Instance::Disk": {
        "WindowsDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mywindowsinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "LogicalDisk % Free Space",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "objectname",
                        "Value": "LogicalDisk"
                    },
                    {
                        "Name": "instance",
                        "Value": "${EC2::Disk::Path}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

Affichage de la configuration de votre Accelerate Alarm Manager

Les AMSManagedalarmes et les alarmes CustomerManagedAlarmspeuvent être consultées AppConfig avec GetConfiguration.

Voici un exemple d'`GetConfiguration`appel :

```
aws appconfig get-configuration --application AMSAlarmManager --environment
 AMSInfrastructure --configuration AMSManagedAlarms --client-id
      any-string outfile.json
```

- Application : il s' AppConfigagit d'une unité logique pour fournir des fonctionnalités ; pour le gestionnaire d'alarmes, c'est `AMSAlarmManager`
- Environnement : c'est l' AMSInfrastructure environnement
- Configuration : pour afficher les alarmes de base AMS Accelerate, la valeur est `AMSManagedAlarms` ; pour afficher les définitions des alarmes du client, la configuration est `CustomerManagedAlarms`
- ID client : il s'agit d'un identifiant unique d'instance d'application, qui peut être n'importe quelle chaîne
- Les définitions des alarmes peuvent être consultées dans le fichier de sortie spécifié, qui dans ce cas est `outfile.json`

Vous pouvez voir quelle version de configuration est déployée sur votre compte en consultant les déploiements antérieurs dans l' AMSInfrastructureenvironnement.

Modification de la configuration de l'alarme Accelerate

Pour ajouter ou mettre à jour de nouvelles définitions d'alarme, vous pouvez déployer le document Utilisation AWS CloudFormation pour déployer Accélérer les modifications de configuration de configuration ou appeler l'CreateHostedConfigurationVersionAPI.

Il s'agit d'une commande de ligne de commande Linux qui génère la valeur du paramètre en base64, ce que la commande AppConfig CLI attend. Pour plus d'informations, consultez la AWS CLI documentation Binary/Blob (gros objet binaire).

À titre d'exemple :

```
aws appconfig create-hosted-configuration-version --application-id application-id --
configuration-profile-id configuration-profile-id --content base64-string
```

```
      --content-type application/json
```

- ID de l'application : ID de l'application AMS AlarmManager ; vous pouvez le découvrir grâce à l'appel ListApplicationsd'API.
- ID du profil de configuration : ID de la configuration CustomerManagedAlarms ; vous pouvez le découvrir grâce à l'appel ListConfigurationProfilesd'API.
- Contenu : chaîne Base64 du contenu, à créer en créant un document et en l'encodant en base64 : cat alarms-v2.json | base64 (voir Binary/Blob (binary large object)).

  Type de contenu : type MIME, `application/json` car les définitions d'alarme sont écrites en JSON.

> **Important**
>
> Limitez l'accès aux actions StartDeploymentet aux StopDeploymentAPI aux utilisateurs de confiance qui comprennent les responsabilités et les conséquences du déploiement d'une nouvelle configuration sur vos cibles.

Pour en savoir plus sur l'utilisation des AppConfig fonctionnalités AWS pour créer et déployer une configuration, consultez Travailler avec AWS AppConfig.

Modification de la configuration par défaut de l'alarme Accelerate

Bien que vous ne puissiez pas modifier le profil de configuration par défaut, vous pouvez remplacer les paramètres par défaut en spécifiant un bloc de configuration dans votre profil de personnalisation avec le même identifiant de configuration que le bloc de configuration par défaut. Dans ce cas, l'ensemble de votre bloc de configuration remplace le bloc de configuration par défaut pour lequel la configuration de balisage doit s'appliquer.

Par exemple, considérez le profil de configuration par défaut suivant :

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
```

```
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 5,
                ...
            }
        }
    }
}
```

Pour modifier le seuil de cette alarme à 10, vous devez fournir la définition complète de l'alarme, et pas uniquement les parties que vous souhaitez modifier. Par exemple, vous pouvez fournir le profil de personnalisation suivant :

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 10,
                ...
            }
```

```
        }
    }
}
```

> **Important**
>
> N'oubliez pas de déployer vos modifications de configuration une fois que vous les avez apportées. Dans SSM AppConfig, vous devez déployer une nouvelle version de la configuration après l'avoir créée.

Déploiement Accélérez les modifications de configuration des

Une fois la personnalisation terminée, vous devez la déployer, avec AppConfig ou AWS CloudFormation.

Rubriques

- Utilisation AppConfig pour déployer Accelerate les modifications de configuration des alarmes
- Utilisation AWS CloudFormation pour déployer Accélérer les modifications de configuration

Utilisation AppConfig pour déployer Accelerate les modifications de configuration des alarmes

Une fois la personnalisation terminée, utilisez-le AppConfig pour déployer vos modifications avec StartDeployment.

```
  aws appconfig start-deployment --application-id application_id
   --environment-id environment_id Vdeployment-strategy-id
   deployment_strategy_id --configuration-profile-id configuration_profile_id --
configuration-version 1
```

- ID de l'application : ID de l'application`AMSAlarmManager`, vous pouvez le trouver dans l'appel ListApplicationsd'API.
- ID d'environnement : vous pouvez le trouver dans l'appel ListEnvironmentsd'API.
- ID de stratégie de déploiement : vous pouvez le trouver dans l'appel ListDeploymentStrategiesd'API.
- ID du profil de configuration : ID de `CustomerManagedAlarms` ; vous pouvez le trouver dans l'appel ListConfigurationProfilesd'API.

- Version de configuration : version du profil de configuration à déployer.

> **Important**
>
> Alarm Manager applique les définitions d'alarme telles que spécifiées dans les profils de configuration. Toutes les modifications manuelles que vous apportez aux CloudWatch alarmes avec le CloudWatch CLI/SDK AWS Management Console ou le CLI/SDK sont automatiquement annulées. Assurez-vous donc que vos modifications sont définies via Alarm Manager. Pour comprendre quelles alarmes sont créées par le gestionnaire d'alarmes, vous pouvez rechercher la `ams:alarm-manager:managed` balise avec une valeur`true`. Limitez l'accès aux actions StartDeploymentet aux StopDeploymentAPI aux utilisateurs de confiance qui comprennent les responsabilités et les conséquences du déploiement d'une nouvelle configuration sur vos cibles.

Pour en savoir plus sur l'utilisation des AppConfig fonctionnalités AWS pour créer et déployer une configuration, consultez la AppConfig documentation AWS.

Utilisation AWS CloudFormation pour déployer Accélérer les modifications de configuration

Si vous souhaitez déployer votre profil de `CustomerManagedAlarms` configuration à l'aide des modèles suivants AWS CloudFormation, vous pouvez utiliser les AWS CloudFormation modèles suivants. Entrez la configuration JSON souhaitée dans le `AMSAlarmManagerConfigurationVersion.Content` champ.

Lorsque vous déployez les modèles dans une AWS CloudFormation pile ou un ensemble de piles, le déploiement de la `AMSResourceTaggerDeployment` ressource échoue si vous n'avez pas suivi le format JSON requis pour la configuration. Voir Accélérer le profil de configuration : surveillance pour plus de détails sur le format attendu.

Pour obtenir de l'aide sur le déploiement de ces modèles sous forme de CloudFormation pile ou d'ensemble de piles, consultez la CloudFormation documentation AWS correspondante ci-dessous :

- Création d'une pile sur la CloudFormation console AWS
- Création d'une pile avec l'AWS CLI
- Création d'un ensemble de piles

> **Note**
>
> Si vous déployez une version de configuration à l'aide de l'un de ces modèles, puis que vous supprimez ensuite l'ensemble CloudFormation de piles ou de piles, la version de configuration du modèle restera la version actuellement déployée et aucun déploiement supplémentaire ne sera effectué. Si vous souhaitez revenir à une configuration par défaut, vous devez soit déployer manuellement une configuration vide (c'est-à-dire juste {}), soit mettre à jour votre pile avec une configuration vide, plutôt que de supprimer la pile.

JSON

```
{
  "Description": "Custom configuration for the AMS Alarm Manager.",
  "Resources": {
    "AMSAlarmManagerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "Content": "{}",
        "ContentType": "application/json"
      }
    },
    "AMSAlarmManagerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSAlarmManagerConfigurationVersion"
        },
```

```
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Alarm Manager.
Resources:
  AMSAlarmManagerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      Content: |
        {

        }
      ContentType: application/json
  AMSAlarmManagerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      ConfigurationVersion:
        !Ref AMSAlarmManagerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-Alarm-Manager-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-Alarm-Manager-Configuration-EnvironmentId
```

Annulation accélérée des changements d'alarme

Vous pouvez annuler les définitions d'alarme par le biais du même mécanisme de déploiement en spécifiant une version de profil de configuration précédente et en l'exécutant StartDeployment.

Conserver les alarmes Accel

Lorsque les ressources surveillées par AMS sont supprimées, toutes les alarmes créées par Alarm Manager pour ces ressources sont automatiquement supprimées par Alarm Manager. Si vous devez conserver certaines alarmes à des fins d'audit, de conformité ou d'historique, utilisez la fonction de mémorisation des balises d'Alarm Manager.

Pour conserver une alarme même après la suppression de sa ressource surveillée, ajoutez une `"ams:alarm-manager:retain"` balise à la configuration personnalisée de l'alarme, comme indiqué dans l'exemple suivant.

```
{
  "AWS::EC2::Instance": {
    "AMSCpuAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:ams-monitoring-policy",
        "Value": "ams-monitored"
      },
      "AlarmDefinition": {
        "AlarmName": "${EC2::InstanceId}: CPU Too High",
        "AlarmDescription": "AMS Baseline Alarm for EC2 CPUUtilization",
        [...]
        "Tags": [
          {
            "Key": "ams:alarm-manager:retain",
            "Value": "true"
          }
        ]
      }
    }
  }
}
```

Une alarme configurée avec le `"ams:alarm-manager:retain"` tag n'est pas automatiquement supprimée par Alarm Manager lorsque la ressource surveillée est interrompue. L'alarme conservée

persiste CloudWatch indéfiniment jusqu'à ce que vous la supprimiez manuellement à l'aide de CloudWatch.

Désactivation de la configuration d'alarme Accelerate par défaut

AMS Accelerate fournit le profil de configuration par défaut de votre compte en fonction des alarmes de base. Toutefois, cette configuration par défaut peut être désactivée en remplaçant l'une des définitions d'alarme. Vous pouvez désactiver une règle de configuration par défaut en remplaçant l'ID de configuration de la règle dans votre profil de configuration de personnalisation et en spécifiant le champ activé avec la valeur false.

Par exemple, si la configuration suivante était présente dans le profil de configuration par défaut :

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                ...
            }
        }
    }
```

Vous pouvez désactiver cette règle de balisage en incluant les éléments suivants dans votre profil de configuration de personnalisation :

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": false
        }
    }
}
```

Pour effectuer ces modifications, l'CreateHostedConfigurationVersionAPI doit être appelée avec le document de profil JSON (voirModification de la configuration de l'alarme Accelerate) et doit

ensuite être déployée (voirDéploiement Accélérez les modifications de configuration des). Notez que lorsque vous créez la nouvelle version de configuration, vous devez également inclure les alarmes personnalisées que vous souhaitez créer précédemment dans le document de profil JSON.

> **Important**
>
> Lorsqu'AMS Accelerate met à jour le profil de configuration par défaut, celui-ci n'est pas calibré par rapport aux alarmes personnalisées que vous avez configurées. Vérifiez donc les modifications apportées aux alarmes par défaut lorsque vous les remplacez dans votre profil de configuration personnalisé.

Création d' CloudWatch alarmes supplémentaires pour Accelerate

Vous pouvez créer des CloudWatch alarmes supplémentaires pour AMS Accelerate à l'aide de CloudWatch métriques et d'alarmes personnalisées pour les EC2 instances Amazon.

Produisez votre script de surveillance des applications et vos métriques personnalisées. Pour plus d'informations et pour accéder à des exemples de scripts, consultez la section Surveillance des métriques de mémoire et de disque pour les instances Amazon EC2 Linux.

Les scripts CloudWatch de surveillance pour les EC2 instances Amazon Linux montrent comment produire et utiliser des CloudWatch métriques personnalisées. Ces exemples de scripts Perl comportent un exemple entièrement fonctionnel qui indique les métriques d'utilisation de la mémoire, des échanges et de l'espace sur le disque pour une instance Linux.

> **Important**
>
> AMS Accelerate ne surveille pas les CloudWatch alarmes que vous avez créées.

Affichage du nombre de ressources surveillées par Alarm Manager pour Accelerate

Alarm Manager envoie des métriques toutes les heures à Amazon CloudWatch, dans l'espace de `AMS/AlarmManager` noms. Les métriques sont émises uniquement pour les types de ressources pris en charge par Alarm Manager.

Nom de la métrique	Dimensions	Description
ResourceCount	Composant, ResourceType	Nombre de ressources (du type de ressource spécifié) déployées dans cette région. Unités : nombre
ResourcesMissingManagedAlarms	Composant, ResourceType	Nombre de ressources (du type de ressource spécifié) qui nécessitent des alarmes gérées, mais Alarm Manager n'a pas encore appliqué les alarmes. Unités : nombre
UnmanagedResources	Composant, ResourceType	Nombre de ressources (du type de ressource spécifié) auxquelles aucune alarme gérée n'est appliquée par Alarm Manager. Généralement, ces ressources ne correspondent à aucun bloc de configuration d'Alarm Manager ou sont explicitement exclues des blocs de configuration. Unités : nombre
MatchingResourceCount	Composant ResourceType, ConfigClauseName	Nombre de ressources (du type de ressource spécifié) correspondant au bloc de configuration d'Alarm Manager. Pour qu'une ressource corresponde au bloc de configuration, le bloc doit être activé et la ressource doit avoir les mêmes balises que celles spécifiées dans le bloc de configuration. Unités : nombre

Ces statistiques sont également consultables sous forme de graphiques, dans le tableau de bord AMS-Alarm-Manager-Reporting-Dashboard. Pour voir le tableau de bord, depuis la console de AWS CloudWatch gestion, sélectionnez AMS-Alarm-Manager-Reporting-Dashboard. Par défaut, les graphiques de ce tableau de bord affichent les données de la période de 12 heures précédente.

AMS Accelerate déploie des CloudWatch alarmes sur votre compte afin de détecter les augmentations significatives du nombre de ressources non gérées, par exemple les ressources exclues de la gestion par AMS Alarm Manager. AMS Operations étudiera les augmentations des ressources non gérées qui dépassent : soit trois ressources du même type, soit une augmentation de 50 % par rapport à toutes les ressources du même type. Si le changement ne semble pas être délibéré, AMS Operations peut vous contacter pour examiner le changement.

Correction automatique des alertes par AMS

Après vérification, AWS Managed Services (AMS) corrige automatiquement certaines alertes en fonction des conditions et des processus spécifiques décrits dans cette section.

Nom de l'alerte	Description	Seuils	Action
Échec de la vérification du statut	Défaillances matérielles possibles ou état défaillant de l'instance.	Le système a détecté un état défaillant au moins une fois au cours des 15 dernières minutes.	La correction automatique AMS valide d'abord si l'instance est accessible. Si l'instance est inaccessible, elle est arrêtée puis redémarrée. L'arrêt et le démarrage permettent à l'instance de migrer vers le nouveau matériel sous-jacent. Pour plus d'informations, consultez la section suivante « Automatisation de la correction des défaillances lors de la vérification de l'EC2 état ».
AMSLinuxDiskUsage	Déclenchez lorsque l'utilisation du disque d'un point de montage (espace désigné sur un volume)	Le seuil est supérieur à la valeur définie 6 fois au cours des 30 dernières minutes.	La correction automatique AMS supprime d'abord les fichiers temporaires. Si cela ne permet pas de libérer suffisamment

Nom de l'alerte	Description	Seuils	Action
	sur votre EC2 instance est pleine.		d'espace disque, cela augmente le volume afin d'éviter toute interrupt ion de service en cas de saturation du volume.
AMSWindow sDiskUsag e	Lorsque l'utilisation du disque d'un point de montage (espace désigné sur un volume) sur votre EC2 instance est épuisée.	Le seuil est supérieur à la valeur définie 6 fois au cours des 30 dernières minutes.	La correction automatiq ue AMS supprime d'abord les fichiers temporaires. Si cela ne permet pas de libérer suffisamment d'espace disque, cela augmente le volume afin d'éviter toute interrupt ion de service en cas de saturation du volume.

Nom de l'alerte	Description	Seuils	Action
RDS-EVENT-0089	L'instance de base de données a consommé plus de 90 % de son stockage alloué.	Le stockage est alloué à plus de 90 %.	La correction automatique AMS valide d'abord que la base de données est dans un état modifiable et disponible ou qu'elle est pleine en stockage. Il tente ensuite d'augmenter le stockage alloué, le nombre d'E/S par seconde et le débit de stockage par le biais d'un CloudFormation ensemble de modifications. Si une dérive de pile est déjà détectée, elle revient à l'API RDS pour éviter les temps d'arrêt. Cette fonctionnalité peut être désactivée en ajoutant la balise suivante à l'instance de base de données RDS : `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

Nom de l'alerte	Description	Seuils	Action
RDS-EVENT-0007	Le stockage alloué à l'instance de base de données est épuisé. Pour résoudre le problème, allouez de l'espace de stockage supplémentaire.	Le stockage est alloué à 100 %.	La correction automatique AMS valide d'abord que la base de données est dans un état modifiable et disponible ou qu'elle est pleine en stockage. Il tente ensuite d'augmenter le stockage alloué, le nombre d'E/S par seconde et le débit de stockage par le biais d'un CloudFormation ensemble de modifications. Si une dérive de pile est déjà détectée, elle revient à l'API RDS pour éviter les temps d'arrêt. Cette fonctionnalité peut être désactivée en ajoutant la balise suivante à l'instance de base de données RDS : `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

Nom de l'alerte	Description	Seuils	Action
RDS-EVENT-0224	Le stockage alloué demandé atteint ou dépasse le seuil de stockage maximal configuré.	Le seuil de stockage maximal pour l'instance de base de données a été dépassé ou est supérieur ou égal au stockage alloué demandé.	La correction automatique AMS valide d'abord que la quantité de stockage RDS demandée dépassera le seuil de stockage maximal. En cas de confirmation, AMS tente d'augmenter le seuil de stockage maximal de 30 % à l'aide d'un CloudFormation ensemble de modifications ou d'une API RDS directe si les ressources ne sont pas provisionnées par le biais d'un ensemble de modifications. CloudFormation Cette fonctionnalité peut être désactivée en ajoutant la balise suivante à l'instance de base de données RDS : `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

Nom de l'alerte	Description	Seuils	Action
Capacité de stockage RDS	Il reste moins de 1 Go dans le stockage alloué à l'instance de base de données.	Le stockage est alloué à 99 %.	La correction automatique AMS valide d'abord que la base de données est dans un état modifiable et disponible ou qu'elle est pleine en stockage. Il tente ensuite d'augmenter le stockage alloué, le nombre d'E/S par seconde et le débit de stockage par le biais d'un CloudFormation ensemble de modifications. Si une dérive de pile est déjà détectée, elle revient à l'API RDS pour éviter les temps d'arrêt. Cette fonctionnalité peut être désactivée en ajoutant la balise suivante à l'instance de base de données RDS : `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

EC2 échec de la vérification de l'état : notes sur l'automatisation des mesures correctives

Comment fonctionne la correction automatique AMS en cas d'échec EC2 du contrôle d'état :

- Si votre EC2 instance Amazon est devenue inaccessible, elle doit être arrêtée et redémarrée afin de pouvoir être migrée vers un nouveau matériel et récupérée.
- Si l'origine du problème se trouve dans le système d'exploitation (périphériques manquants dans fstab, corruption du noyau, etc.), l'automatisation n'est pas en mesure de récupérer votre instance.
- Si votre instance appartient à un groupe Auto Scaling, l'automatisation ne prend aucune mesure : AutoScalingGroup l'action de dimensionnement remplace l'instance.
- Si la restauration EC2 automatique est activée sur votre instance, la correction n'intervient pas.

EC2 automatisation de la correction de l'utilisation des volumes

Comment fonctionne la correction automatique d'AWS Managed Services (AMS) en cas de problèmes d'utilisation des EC2 volumes :

- L'automatisation valide d'abord si l'extension du volume est requise et si elle peut être réalisée. Si l'extension est jugée appropriée, l'automatisation peut augmenter la capacité du volume. Ce processus automatisé équilibre le besoin de croissance avec une expansion contrôlée et limitée.
- Avant d'étendre un volume, l'automatisation exécute des tâches de nettoyage (Windows : Disk Cleaner, Linux : Logrotate + Simple Service Manager Agent Log removal removal) sur l'instance pour essayer de libérer de l'espace.

> **Note**
>
> Les tâches de nettoyage ne sont pas exécutées sur les instances de la famille EC2 « T » car elles dépendent des crédits du processeur pour garantir le fonctionnement continu.

- Sous Linux, l'automatisation prend uniquement en charge l'extension des systèmes de fichiers de type A EXT2 EXT3, EXT4 et XFS.
- Sous Windows, l'automatisation prend uniquement en charge le système de fichiers NTFS (New Technology File System) et le système de fichiers résilient (ReFS).
- L'automatisation n'étend pas les volumes qui font partie du Logical Volume Manager (LVM) ou d'une matrice RAID.
- L'automatisation n'augmente pas les volumes de stockage des instances.
- L'automatisation n'intervient pas si le volume concerné est déjà supérieur à 2 TiB.
- L'extension par le biais de l'automatisation est limitée à un maximum de trois fois par semaine et à cinq fois au total pendant la durée de vie du système.

- L'automatisation n'augmente pas le volume si l'extension précédente a eu lieu au cours des six dernières heures.

Lorsque ces règles empêchent l'automatisation de prendre des mesures, AMS vous contacte par le biais d'une demande de service sortante afin de déterminer les prochaines actions à entreprendre.

Automatisation de la correction des événements liés à un faible niveau de stockage sur Amazon RDS

Comment fonctionne la correction automatique d'AWS Managed Services (AMS) en cas de faible capacité de stockage sur Amazon RDS :

- Avant d'essayer d'étendre le stockage de l'instance Amazon RDS, l'automatisation effectue plusieurs vérifications pour s'assurer que l'instance Amazon RDS est dans un état modifiable et disponible, ou qu'elle est pleine.
- Lorsqu' CloudFormation une dérive de pile est détectée, la correction est effectuée via l'API Amazon RDS.
- L'action de correction ne s'exécute pas dans les scénarios suivants :
  - Le statut de l'instance Amazon RDS n'est pas « disponible » ou « plein ».
  - Le stockage des instances Amazon RDS n'est actuellement pas modifiable (par exemple lorsque le stockage a été modifié au cours des six dernières heures).
  - Le stockage auto-scaling est activé sur l'instance Amazon RDS.
  - L'instance Amazon RDS n'est pas une ressource au sein d'une CloudFormation pile.
- Les mesures correctives sont limitées à une extension toutes les six heures et au maximum à trois extensions par période continue de quatorze jours.
- Lorsque ces scénarios se produisent, AMS vous contacte pour vous signaler un incident sortant afin de déterminer les prochaines actions.

Utilisation des règles EventBridge gérées par Amazon dans AMS

AMS Accelerate utilise les règles EventBridge gérées par Amazon. Une règle gérée est un type unique de règle directement lié à AMS. Ces règles correspondent aux événements entrants et les envoient aux cibles pour traitement. Les règles gérées sont prédéfinies par AMS et incluent des modèles d'événements requis par le service pour gérer les comptes clients. Sauf indication contraire, seul le service propriétaire peut utiliser ces règles gérées.

Les règles gérées par AMS Accelerate sont liées au principal `events.managedservices.amazonaws.com` de service. Ces règles gérées sont gérées via le rôle `AWSServiceRoleForManagedServices_Events`lié au service. Pour supprimer ces règles, une confirmation spéciale du client est requise. Pour plus d'informations, voir Supprimer les règles gérées pour AMS.

Pour plus d'informations sur les règles, consultez la section Règles du guide de EventBridge l'utilisateur Amazon.

Amazon EventBridge Managed Rules déployées par AMS

Règles EventBridge gérées par Amazon

Nom de règle	Description	Définition

AmsAccessRolesRule	Cette règle tient compte des modifications apportées aux rôles et politiques spécifiques d'AMS Accelerate.	{
		"source": ["aws.iam"],
		"detail-type": ["AWS API Call via CloudTrail"],
		"detail": {
		"eventName": [
		"DeleteRole",
		"DeletePolicy",
		"CreatePolicyVersion",
		"AttachRolePolicy",
		"DetachRolePolicy"
		],
		"requestParameters": {
		"$or": [
		{
		"roleName": [
		"ams-access-admin",
		"ams-access-admin-operations",
		"ams-access-operations",
		"ams-access-read-only",
		"ams-access-security-analyst",
		"ams-access-security-analyst-read-only"
		]
		},
		{
		"policyArn": [

Nom de règle	Description	Définition

```
                    "arn:*:iam::*:policy/ams-ac
cess-allow-pass-role",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-cloudshell-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-operations-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-update-iam-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-ssr-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-read-only-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-extended-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-admin-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-admin-operations-policy"
                ]
            },
         ]
       },
   },
}
```

Nom de règle	Description	Définition

AMSCoreRègle	Cette règle transmet AWS Config les CloudWatch événements Amazon aux services de correction AMS Config et de surveillance AMS de manière respectueuse. Les AWS Config événements créent et résolvent AWS Systems Manager OpsItems. Les CloudWatch événements Amazon surveillent les CloudWatch alarmes.	<pre>{
		    {
		        "source": ["aws.config", "aws.cloudwatch"],
		        "detail-type": ["Config Rules Compliance Change", "CloudWatch Alarm State Change"],
		    }
		}</pre>

Création de règles gérées pour AMS

Il n'est pas nécessaire de créer manuellement les Amazon EventBridge Managed Rules. Lorsque vous intégrez AMS dans la console AWS de gestion AWS CLI, l'API ou l' AWS API, AMS les crée pour vous.

Modification des règles gérées pour AMS

AMS ne vous permet pas de modifier les règles gérées. Le nom et le modèle d'événement de chaque règle gérée sont prédéfinis par AMS.

Suppression de règles gérées pour AMS

Il n'est pas nécessaire de supprimer manuellement les règles gérées. Lorsque vous quittez AMS dans la console de AWS gestion AWS CLI, l'API ou l' AWS API, AMS nettoie les ressources et supprime pour vous toutes les règles gérées détenues par AMS.

Si AMS ne parvient pas à supprimer les règles gérées lors de l'offboarding, vous pouvez également utiliser la EventBridge console Amazon, l'API AWS CLI ou l' AWS API pour supprimer manuellement les règles gérées. Pour ce faire, vous devez d'abord quitter AMS et procéder à une suppression forcée des règles gérées.

Remédiateur fiable dans AMS

Trusted Remediator est une solution AWS Managed Services qui automatise la correction et les recommandations. AWS Trusted AdvisorAWS Compute Optimizer Trusted Remediator émet des recommandations lorsque Trusted Advisor et Compute Optimizer vous indique des opportunités de réduction des coûts, d'amélioration de la disponibilité du système, d'optimisation des performances ou de correction des failles de sécurité de votre entreprise. Comptes AWS Avec Trusted Remediator, vous pouvez répondre à ces recommandations en matière de sécurité, de performance, d'optimisation des coûts, de tolérance aux pannes et de limites de service d'une manière sûre et standardisée en utilisant les meilleures pratiques établies. Trusted Remediator vous permet de configurer une solution de correction et s'exécute automatiquement selon un calendrier que vous créez, ce qui simplifie le processus de correction. Cette approche rationalisée permet de résoudre les problèmes de manière cohérente, efficace et sans intervention manuelle.

Principaux avantages de Trusted Remediator

Les principaux avantages de Trusted Remediator sont les suivants :

- Amélioration de la sécurité, des performances et de l'optimisation des coûts : Trusted Remediator vous aide à améliorer le niveau de sécurité global de vos comptes, à optimiser l'utilisation des ressources et à réduire les coûts opérationnels.
- Configuration et configuration en libre-service : vous pouvez configurer Trusted Remediator en fonction de vos besoins et préférences.
- Trusted Advisor Contrôles automatisés et correction AWS Compute Optimizer des recommandations : après la configuration, Trusted Remediator exécute automatiquement les actions de correction pour les contrôles sélectionnés. Cette automatisation élimine le besoin d'intervention manuelle.
- Mise en œuvre des meilleures pratiques : les mesures correctives sont basées sur les meilleures pratiques établies, de sorte que les problèmes sont traités de manière standardisée et efficace.
- Exécution planifiée : vous pouvez choisir le calendrier de correction qui correspond à vos flux de travail day-to-day opérationnels.

Trusted Remediator vous permet de résoudre de manière proactive les problèmes identifiés dans vos AWS environnements, en vous aidant à respecter les meilleures pratiques et à maintenir une infrastructure cloud sécurisée, performante et rentable.

Comment fonctionne Trusted Remediator

Voici une illustration du flux de travail Trusted Remediator :

Trusted Remediator évalue Trusted Advisor et recommande Compute Optimizer pour Comptes AWS vous et crée. AWS Systems Manager OpsItems OpsCenter Vous pouvez ensuite utiliser les documents d'automatisation de Trusted Remediator pour y remédier OpsItems automatiquement ou manuellement. Vous trouverez ci-dessous des informations détaillées pour chaque type de correction :

- Correction automatisée : Trusted Remediator exécute le document d'automatisation et surveille l'exécution. Une fois le document d'automatisation terminé, Trusted Remediator résout l'Opsitem.
- Correction manuelle : Trusted Remediator crée le OpsItem fichier que vous pouvez consulter. Après avoir révisé, vous pouvez démarrer le document d'automatisation.

Les journaux de correction sont stockés dans un compartiment Amazon S3. Vous pouvez utiliser les données du compartiment S3 pour créer des QuickSight tableaux de bord personnalisés pour les

rapports. AMS fournit également des rapports sur demande pour Trusted Remediator. Pour recevoir ces rapports, contactez votre CSDM. Pour de plus amples informations, veuillez consulter Rapports Trusted Remediator.

Termes clés pour Trusted Remediator

Les termes suivants sont utiles à connaître lorsque vous utilisez Trusted Remediator dans AMS :

- AWS Trusted Advisor et AWS Compute Optimizer : Services d'optimisation du cloud fournis par AWS. Trusted Advisor et Compute Optimizer inspectent votre AWS environnement et fournissent des recommandations basées sur les meilleures pratiques dans les six catégories suivantes :
  - Optimisation des coûts
  - Performances
  - Sécurité
  - Tolérance aux pannes
  - Excellence opérationnelle
  - Service Limits

  Pour plus d'informations, consultez AWS Trusted Advisor et AWS Compute Optimizer.
- Trusted Remediator : solution de correction AMS pour les Trusted Advisorvérifications et AWS Compute Optimizerles recommandations. Trusted Remediator vous aide à corriger en toute sécurité les Trusted Advisor vérifications et les recommandations de Compute Optimizer à l'aide des meilleures pratiques connues afin d'améliorer la sécurité, les performances et de réduire les coûts. Trusted Remediator est facile à installer et à configurer. Vous configurez une seule fois, et Trusted Remediator exécute les corrections selon le calendrier de votre choix (quotidien ou hebdomadaire).
- AWS Systems Manager Document SSM : fichier JSON ou YAML qui définit les actions effectuées sur AWS Systems Manager vos AWS ressources. Le document SSM sert de spécification déclarative pour automatiser les tâches opérationnelles sur plusieurs AWS ressources et instances.
- AWS Systems Manager OpsCenter OpsItem: ressource de gestion des problèmes opérationnels dans le cloud qui vous aide à suivre et à résoudre les problèmes opérationnels dans votre AWS environnement. OpsItems fournir une vue et un système de gestion centralisés pour les données opérationnelles et les problèmes Services AWS liés aux ressources. Chacun OpsItem représente un problème opérationnel, tel qu'un risque de sécurité potentiel, un problème de performance ou un incident opérationnel.

- Configuration : Une configuration est un ensemble d'attributs stockés dans AWS AppConfig, une capacité de AWS Systems Manager. L'application Trusted Remediator AWS AppConfig permet de configurer les mesures correctives au niveau du compte. Vous pouvez utiliser la AWS AppConfig console ou l'API pour modifier les configurations.
- Mode d'exécution : le mode d'exécution est un attribut de configuration qui détermine la manière d'exécuter la correction pour chaque résultat de Trusted Advisor vérification. Quatre modes d'exécution sont pris en charge : automatique, manuel, conditionnel et inactif.
- Remplacer les ressources : cette fonctionnalité utilise des balises de ressources pour remplacer une configuration pour des ressources spécifiques.
- Journal des éléments de correction : fichier journal situé dans le compartiment journal S3 de correction de Trusted Remediator. Le journal des éléments de correction est créé lors de la création des mesures correctives. OpsItems Ce fichier journal contient la correction d'exécution manuelle OpsItems et la correction OpsItems d'exécution automatique. Utilisez ce fichier journal pour suivre tous les éléments de correction.
- Journal d'exécution automatique des mesures correctives : fichier journal situé dans le compartiment journal S3 de correction de Trusted Remediator. Le journal d'exécution automatique des mesures correctives est créé lorsque l'exécution automatique d'un document SSM est terminée. Ce journal contient les détails de l'exécution de SSM pour la correction OpsItems automatique de l'exécution. Utilisez ce fichier journal pour suivre les corrections automatisées.

Commencez avec Trusted Remediator dans AMS

Trusted Remediator est disponible dans AMS sans frais supplémentaires. Trusted Remediator prend en charge les configurations à compte unique et à comptes multiples.

Intégration à Trusted Remediator

Pour intégrer vos comptes AMS à Trusted Remediator, envoyez un e-mail à vos architectes cloud ou à vos responsables de prestation de services cloud (CSDMs). Dans le corps de l'e-ma il, incluez les informations suivantes :

- Comptes AWS: le numéro d'identification du compte à douze chiffres. Tous les comptes que vous souhaitez intégrer à Trusted Remediator doivent appartenir au même client Accelerate.
  - Compte administrateur délégué : compte utilisé pour vérifier la configuration Trusted Advisor d'un ou de plusieurs comptes par Compute Optimizer.

- Comptes de membre : il s'agit des comptes liés au compte d'administrateur délégué. Ces comptes héritent des configurations du compte d'administrateur délégué. Vous pouvez avoir un ou plusieurs comptes membres.

  > **Note**
  >
  > Les comptes membres héritent des configurations du compte d'administrateur délégué. Si vous avez besoin de configurations différentes pour des comptes spécifiques, intégrez plusieurs comptes d'administrateur délégué avec vos configurations préférées. Planifiez la structure du compte et les configurations avec vos architectes cloud avant de vous lancer.

- Régions AWS: l' Régions AWS endroit où se trouvent vos ressources. Pour une liste de Régions AWS, voir Services AWS par région.
- Calendrier et heure des mesures correctives : votre calendrier de remédiation préféré (quotidien ou hebdomadaire). Trusted Remediator collecte les Trusted Advisor vérifications et lance les mesures correctives à l'heure prévue. Par exemple, vous pouvez définir le calendrier des mesures correctives pour 1 h 00 le dimanche de chaque semaine, heure normale de l'est de l'Australie.
- E-mail de notification : Trusted Remediator utilise l'e-mail de notification pour vous informer quotidiennement de la mise en œuvre de mesures correctives. L'objet de l'e-mail de notification est « Résumé des mesures correctives de Trusted Remediator » et le contenu fournit des informations sur les mesures correctives de Trusted Remediator exécutées au cours des dernières 24 heures.

  > **Note**
  >
  > Passez en revue vos applications et vos ressources après chaque correction planifiée. Pour obtenir une assistance supplémentaire, contactez AMS.

Une fois que vous avez soumis votre demande d'intégration avec les informations requises à votre CA ou à votre CSDM, AMS intègre vos comptes à Trusted Remediator. Trusted Remediator utilise AWS AppConfig une fonctionnalité de AWS Systems Manager pour définir la configuration des Trusted Advisor vérifications. Ces configurations sont un ensemble d'attributs qui sont stockés dans AWS AppConfig. Pour éviter que vos ressources ne soient facturées de manière non autorisée, tous les Trusted Advisor chèques pris en charge sont définis sur Inactifs lorsque les comptes sont intégrés à Trusted Remediator. Une fois intégré, vous pouvez utiliser la AWS AppConfig console ou l'API pour gérer les configurations. Ces configurations vous aident à corriger automatiquement

des Trusted Advisor vérifications spécifiques ou à évaluer et corriger manuellement les vérifications restantes. Les configurations sont hautement personnalisables, ce qui vous permet d'appliquer des configurations pour chaque Trusted Advisor contrôle. Pour de plus amples informations, veuillez consulter Configurer Trusted Advisor la correction des chèques dans Trusted Remediator.

Choisissez les vérifications et les recommandations à corriger

Par défaut, le mode d'exécution de la correction est inactif pour toutes les Trusted Advisor vérifications et recommandations de Compute Optimizer dans votre configuration. Cela empêche les mesures correctives non autorisées et protège les ressources. AMS fournit des documents d'automatisation SSM sélectionnés pour la correction des Trusted Advisor chèques.

Pour sélectionner les vérifications que vous souhaitez corriger avec Trusted Remediator, procédez comme suit :

1. Consultez la liste des recommandations prises en charge Trusted Advisor et de Compute Optimizer ou le nom des documents d'automatisation SSM associés pour déterminer les vérifications et les recommandations que vous souhaitez corriger avec Trusted Remediator.
2. Mettez à jour votre configuration pour activer la correction pour les Trusted Advisor vérifications que vous avez sélectionnées. Pour obtenir des instructions sur la manière de sélectionner les chèques, consultezConfigurer Trusted Advisor la correction des chèques dans Trusted Remediator.

Suivez vos mesures correctives dans Trusted Remediator

Une fois que vous avez mis à jour la configuration au niveau du compte, Trusted Remediator crée OpsItems pour chaque correction. Trusted Remediator exécute le document SSM pour une correction automatique OpsItems conformément à votre calendrier de correction. Pour obtenir des instructions sur la façon d'afficher toutes les corrections OpsItems depuis la OpsCenter console Systems Manager, reportez-vous Suivez les mesures correctives dans Trusted Remediator à.

Exécuter des corrections manuelles dans Trusted Remediator

Vous pouvez corriger manuellement les Trusted Advisor contrôles. Lorsque vous lancez une correction manuelle, Trusted Remediator crée une exécution manuelle. OpsItem Vous devez consulter et lancer le document d'automatisation SSM pour corriger le. OpsItems Pour de plus amples informations, veuillez consulter Exécutez des corrections manuelles dans Trusted Remediator.

Recommandations de Compute Optimizer soutenues par Trusted Remediator

Le tableau suivant répertorie les recommandations de Compute Optimizer prises en charge, les documents d'automatisation SSM, les paramètres préconfigurés et le résultat attendu des documents d'automatisation. Passez en revue le résultat attendu pour vous aider à comprendre les risques potentiels en fonction des exigences de votre entreprise avant d'activer un document d'automatisation SSM pour la correction des contrôles.

Assurez-vous que la règle de configuration correspondante pour chaque vérification Compute Optimizer est présente pour les vérifications prises en charge pour lesquelles vous souhaitez activer la correction. Pour plus d'informations, voir Accepter AWS Compute Optimizer les Trusted Advisor chèques.

Option d'optimisation	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Redimensionnement		
Recommandations relatives aux EC2 instances Amazon	AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation Type d' EC2 instance Amazon mis à jour conformément aux recommandations de Compute Optimizer. Les options les plus optimales sont choisies tout en conservant les mêmes paramètres de plate-forme (architecture, hyperviseur, interface réseau, type de virtualisation, etc.) si l'option existe.	• MinimumDaysSinceLastChange: paramètre permettant de spécifier le nombre minimum de jours écoulés depuis le dernier changement de type d'instance. La durée par défaut est de 7 jours. Aucune contrainte • Créer un AMIBefore redimensionnement : pour créer l'AMI de l'instance en tant que sauvegarde avant le redimensionnement, définissez le paramètre sur « True ». Pour ne pas créer de sauvegarde, définissez le paramètre sur « False ». La valeur par défaut est « True ».

Option d'optimisation	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
		Aucune contrainte

Option d'optimisation	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Recommandations relatives aux volumes Amazon EBS	AWSManagedServices-ModifyEBSVolume Le volume Amazon EBS est modifié conformément aux recommandations de Compute Optimizer. La modification peut inclure le type de volume, la taille, les IOPS, la génération de volume (gp2, gp3, etc.).	• CreateSnapshot: pour créer un instantané avant de modifier le volume, réglez sur « True ». Pour ne pas créer de capture instantanée, définissez le paramètre sur « Faux ». La valeur par défaut est « True ». Aucune contrainte • VolumeType: le type de volume souhaité. Si aucun type n'est spécifié, le type existant est conservé. Aucune contrainte • VolumeSize: taille souhaitée du volume, en GiB. La taille du volume cible doit être supérieure ou égale à la taille existante du volume. Si aucune taille n'est spécifiée, la taille existante est conservée. Aucune contrainte • IOPS : nombre d' I/O opérations par seconde (IOPS) demandé. Ce paramètre n'est valide que pour les volumes io1, io2 et gp3. Aucune contrainte • Débit : débit à provisionner pour un volume, avec un maximum de 1 000 Mbits/s. Ce paramètre n'est valide que pour les volumes gp3.

Option d'optimisation	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
		Aucune contrainte • RemediateStackDrift: Pour lancer la correction de la dérive, si une dérive est causée par une modification du volume, réglez sur « True ». Pour ne pas tenter de corriger la dérive, définissez le paramètre sur « False ». La valeur par défaut est « True ». Aucune contrainte
Recommandations relatives à la fonction Lambda	AWSManagedServices-TrustedRemediatorOptimizeLambdaMemory AWS Lambda mémoire fonctionnelle optimisée conformément aux recommandations de Compute Optimizer.	RecommendedMemorySize : taille de mémoire personnalisée, si elle est différente des options recommandées. Aucune contrainte
Ressources inutilisées		

Option d'optimisation	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Volume Amazon EBS inactif	AWSManagedServices-DeleteUnusedEBSVolume Le volume Amazon EBS non connecté sera supprimé.	• CreateSnapshot: pour créer un instantané avant de supprimer le volume, réglez sur « True ». Pour ne pas créer de capture instantanée, définissez le paramètre sur « Faux ». La valeur par défaut est « True ». Aucune contrainte • MinimumUnattachedDays: durée minimale de suppression du volume Amazon EBS sans connexion, jusqu'à 62 jours. La valeur par défaut est 7. Aucune contrainte
EC2 Instance Amazon inactive	AWSManagedServices-StopEC2 instances L' EC2 instance Amazon inactive sera arrêtée.	ForceStopWithInstanceStore: Pour forcer l'arrêt des instances utilisant le stockage d'instance, définissez le paramètre sur « True ». Pour ne pas forcer l'arrêt, réglez-le sur « False ». La valeur par défaut « False » empêche l'arrêt de l'instance. Aucune contrainte

Option d'optimisation	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Instance Amazon RDS inactive	AWSManagedServices-StopIdleRDSInstance Arrêtez une instance Amazon RDS inactive. Les moteurs pris en charge sont : MariaDB, Microsoft SQL Server, MySQL, Oracle, PostgreSQL. Ce document ne s'applique pas à Aurora MySQL et Aurora PostgreSQL. L'instance sera arrêtée pendant 7 jours au maximum et relancée automatiquement.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Trusted Advisor contrôles pris en charge par Trusted Remediator

Le tableau suivant répertorie les Trusted Advisor contrôles pris en charge, les documents d'automatisation SSM, les paramètres préconfigurés et le résultat attendu des documents d'automatisation. Passez en revue le résultat attendu pour vous aider à comprendre les risques potentiels en fonction des exigences de votre entreprise avant d'activer un document d'automatisation SSM pour la correction des contrôles.

Assurez-vous que la règle de configuration correspondante pour chaque Trusted Advisor vérification est présente pour les vérifications prises en charge pour lesquelles vous souhaitez activer la correction. Pour plus d'informations, voir Afficher AWS Trusted Advisor les contrôles réalisés par AWS Config. Si un check comporte AWS Security Hub des contrôles correspondants, assurez-vous que le contrôle Security Hub est activé. Pour plus d'informations, consultez la section Activation des contrôles dans Security Hub. Pour plus d'informations sur la gestion des paramètres préconfigurés, voir Configure Trusted Advisor check remédiation dans Trusted Remediator.

Trusted Advisor contrôles d'optimisation des coûts pris en charge par Trusted Remediator

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Z4 AUBRNSmz Adresses IP Elastic non associées	AWSManagedServices-TrustedRemediatorReleaseElasticIP Libère une adresse IP élastique qui n'est associée à aucune ressource.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
c18d2gz150 - Instances Amazon arrêtées EC2	AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime - EC2 Les instances Amazon arrêtées pendant un certain nombre de jours sont résiliées.	• Créer une AMIBefore résiliation : pour créer l'AMI de l'instance en tant que sauvegarde avant de mettre fin à l' EC2 instance Amazon, choisissez`true`. Pour ne pas créer de sauvegarde avant de terminer, choisissez`false`. L'argument par défaut est `true`. • AllowedDays: le nombre de jours pendant lesquels l'instance est à l'état arrêté avant d'être résiliée. La valeur par défaut est 30. Aucune contrainte
c18d2gz128 Référentiel Amazon ECR sans politique de cycle de vie configurée	AWSManagedServices-TrustedRemediatorPutECRLifecyclePolicy Crée une politique de cycle de vie pour le référentiel spécifié s'il n'en existe pas déjà une.	ImageAgeLimit: limite d'âge maximale en jours (1 à 365 jours) pour « n'importe quelle » image du référentiel Amazon ECR. Aucune contrainte
DAvU99Dc4C	AWSManagedServices-DeleteUnusedEBSVolume	• CreateSnapshot: si ce paramètre est défini sur`true`, l'automatisation

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Volumes Amazon EBS sous-utilisés	Supprime les volumes Amazon EBS sous-utilisés s'ils n'ont pas été attachés au cours des 7 derniers jours. Un instantané Amazon EBS est créé par défaut.	crée un instantané du volume Amazon EBS avant sa suppression. Le paramètre par défaut est `true`. Les valeurs valides sont `true` et `false` (distinction majuscules et minuscules). • MinimumUnattachedDays: Nombre minimum de jours sans connexion du volume EBS à supprimer, jusqu'à 62 jours. Si cette valeur est définie sur`0`, le document SSM ne vérifie pas la période de non-connexion et supprime le volume s'il est actuellement déconnecté. La valeur par défaut est7. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
hj M8 LMh88u Équilibreurs de charge inactifs	AWSManagedServices-DeleteIdleClassicLoadBalancer Supprime un Classic Load Balancer inactif s'il n'est pas utilisé et qu'aucune instance n'est enregistrée.	IdleLoadBalancerDays: le nombre de jours pendant lesquels le Classic Load Balancer n'a demandé aucune connexion avant de le considérer comme inactif. La valeur par défaut est de sept jours. Si l'exécution automatique est activée, l'automatisation supprime les équilibreurs de charge classiques inactifs s'il n'existe aucune instance principale active. Pour tous les équilibreurs de charge classiques inactifs dotés d'instances de back-end actives, mais dont les instances de back-end ne sont pas saines, la correction automatique n'est pas utilisée et une correction manuelle est OpsItems créée.
Ti39HalfU8 Instances de base de données Amazon RDS inactives	AWSManagedServices-StopIdleRDSInstance L'instance de base de données Amazon RDS qui est restée inactive au cours des sept derniers jours est arrêtée.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
COr6dfpM05 AWS Lambda fonctions surdimensionnées pour la taille de la mémoire	AWSManagedServices-ResizeLambdaMemory AWS Lambda la taille de la mémoire de la fonction est redimensionnée selon la taille de mémoire recommandée fournie par Trusted Advisor.	RecommendedMemorySize: allocation de mémoire recommandée pour la fonction Lambda. La plage de valeurs est comprise entre 128 et 10240. Si la taille de la fonction Lambda a été modifiée avant l'exécution de l'automatisation, les paramètres peuvent être remplacés par cette automatisation par la valeur recommandée par. Trusted Advisor
QCH7DWOuX1 EC2 Instances Amazon à faible taux d'utilisation	AWSManagedServices-StopEC2Instance (document SSM par défaut pour les modes d'exécution automatique et manuel.) EC2 Les instances Amazon à faible taux d'utilisation sont arrêtées.	ForceStopWithInstanceStore: défini sur pour `true` forcer l'arrêt des instances à l'aide du stockage d'instances. Sinon, définissez sur `false`. La valeur par défaut de `false` empêche l'arrêt de l'instance. Les valeurs valides sont vraies ou fausses (distinction majuscules et minuscules). Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfig urés pris en charge
QCH7DWOuX1 EC2 Instances Amazon à faible taux d'utilisation	AWSManagedServices-ResizeIn stanceByOneLevel L' EC2 instance Amazon est redimensionnée selon un type d'instance inférieur dans le même type de famille d'instances. L'instanc e est arrêtée et démarrée pendant l'opération de redimensionnement et revient à son état initial une fois l'exécution du document SSM terminée. Cette automatisation ne prend pas en charge le redimensi onnement des instances qui se trouvent dans un Auto Scaling Group.	• MinimumDaysSinceLastChange: nombre minimum de jours écoulés depuis le dernier changemen t de type d'instance. Si le type d'instance a été modifié dans un délai spécifié, le type d'instance n'est pas modifié. `0`À utiliser pour ignorer cette validation. L’argument par défaut est 7. • Créer un AMIBefore redimensi onnement : pour créer l'AMI de l'instance en tant que sauvegard e avant le redimensionnement, choisissez. `true` Pour ne pas créer de sauvegarde, choisisse z`false`. L’argument par défaut est `false`. Les valeurs valides sont `true` et `false` (distinction majuscules et minuscules). • ResizeIfStopped: Pour procéder au changement de taille de l'instanc e, même si l'instance est dans un état arrêté, choisissez`true`. Pour ne pas redimensionner automatiquement l'instance en cas d'arrêt, choisissez`false`. Les valeurs valides sont `true` et `false` (distinction majuscules et minuscules). Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
QCH7DWOuX1 EC2 Instances Amazon à faible taux d'utilisation	AWSManagedServices-TerminateInstance Les EC2 instances Amazon peu utilisées sont résiliées si elles ne font pas partie d'un groupe Auto Scaling et si la protection contre la résiliation n'est pas activée. Une AMI est créée par défaut.	Créer une AMIBefore résiliation : définissez cette option sur `true` ou pour `false` créer une AMI d'instance en tant que sauvegarde avant de mettre fin à l' EC2 instance. L'argument par défaut est `true`. Les valeurs valides sont `true` et `false` (distinction majuscules et minuscules). Aucune contrainte
G31SQ1E9U Underutilized Amazon Redshift Clusters	AWSManagedServices-PauseRedshiftCluster Le cluster Amazon Redshift est suspendu.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
c1cj39rr6v Configuration incomplète de l'interruption du téléchargement en plusieurs parties sur Amazon S3	AWSManagedServices-TrustedRemediatorEnableS3AbortIncompleteMultipartUpload Le compartiment Amazon S3 est configuré avec une règle de cycle de vie afin d'annuler les téléchargements partitionnés qui restent incomplets après certains jours.	DaysAfterInitiation: le nombre de jours après lesquels Amazon S3 arrête un chargement partitionné incomplet. La valeur par défaut est fixée à 7 jours. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
c1z7kmr00n Recommandations d'Amazon en matière d'optimisation des EC2 coûts pour les instances	Utilisez les recommandations d' EC2 instance Amazon et Idle Amazon EC2 instance fromRecommandations de Compute Optimizer soutenues par Trusted Remediator.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
c1z7kmr02n Recommandations d'optimisation des coûts d'Amazon EBS pour les volumes	Utilisez les recommandations de volume Amazon EBS et Idle Amazon EBS volume from. Recommandations de Compute Optimizer soutenues par Trusted Remediator	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
c1z7kmr03n Recommandations d'optimisation des coûts Amazon RDS pour les instances de base de données	Utilisez une instance Amazon RDS inactive à partir deRecommandations de Compute Optimizer soutenues par Trusted Remediator.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
c1z7kmr05n AWS Lambda recommandations d'optimisation des coûts pour les fonctions	Utilisez les recommandations relatives à la fonction Lambda de. Recommandations de Compute Optimizer soutenues par Trusted Remediator	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Trusted Advisor contrôles de sécurité pris en charge par Trusted Remediator

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
12Fnkpl8Y5 Exposed Access Keys	AWSManagedServices-TrustedRemediatorDeactivateIAMAccessKey La clé d'accès IAM exposée est désactivée.	Aucun paramètre préconfiguré n'est autorisé. Les applications configurées avec une clé d'accès IAM exposée ne peuvent pas s'authentifier.
Hs4Ma3G127 - API Gateway REST et la journalisation de l'exécution de l'API WebSocket doivent être activées AWS Security Hub Contrôle correspondant : APIGateway1.	AWSManagedServices-TrustedRemediatorEnableAPIGateWayExecutionLogging La journalisation de l'exécution est activée au stade de l'API.	LogLevel: niveau de journalisation pour activer la journalisation de l'exécution, `ERROR` - La journalisation n'est activée que pour les erreurs. `INFO` - La journalisation est activée pour tous les événements. Vous devez autoriser API Gateway à lire et à écrire les journaux de votre compte afin CloudWatch d'activer le journal d'exécution. Reportez-vous à la section Configurer la CloudWatch

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
		journalisation pour REST APIs dans API Gateway pour plus de détails.
Hs4Ma3G129 - Le suivi des étapes de l'API REST d'API Gateway doit être activé AWS X-Ray AWS Security Hub Contrôle correspondant : APIGateway3.	AWSManagedServices-EnableApiGateWayXRayTracing Le traçage X-Ray est activé sur la scène de l'API.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
Hs4Ma3G202 - Les données du cache de l'API REST API Gateway doivent être chiffrées au repos AWS Security Hub Chèque correspondant : APIGateway5.	AWSManagedServices-EnableAPIGatewayCacheEncryption Activez le chiffrement au repos pour les données du cache de l'API REST API Gateway si le cache est activé sur le stage de l'API REST API Gateway.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G177 - AWS Security Hub Contrôle correspondant : les groupes de mise à l'échelle automatique associés à un équilibreur de charge doivent utiliser des contrôles de santé de l'équilibreur de charge .1 AutoScaling	AWSManagedServices-TrustedRemediatorEnableAutoScalingGroupELBHealthCheck Les contrôles de santé d'Elastic Load Balancing sont activés pour le groupe Auto Scaling.	HealthCheckGracePeriod: durée, en secondes, pendant laquelle Auto Scaling attend avant de vérifier l'état de santé d'une instance Amazon Elastic Compute Cloud mise en service. L'activation des contrôles de santé d'Elastic Load Balancing peut entraîner le remplacement d'une instance en cours d'exécution si l'un des équilibreurs de charge Elastic Load Balancing attachés au groupe Auto Scaling indique qu'elle est défectueuse. Pour plus d'informations, voir Associer un équilibreur de charge Elastic Load Balancing à votre groupe Auto Scaling
Hs4Ma3G245 - les AWS CloudFormation piles doivent être intégrées à Amazon Simple Notification Service AWS Security Hub Contrôle correspondant : CloudFormation1.	AWSManagedServices-EnableCFNStackNotification Associez une CloudFormation pile à une rubrique Amazon SNS pour recevoir une notification.	Notification ARNs : ARNs les rubriques Amazon SNS à associer aux piles sélectionnées CloudFormation . Pour activer la correction automatique, le paramètre `NotificationARNs` préconfiguré doit être fourni.

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G210 - CloudFront la journalisation des distributions doit être activée AWS Security Hub Contrôle correspondant : CloudFront2.	AWSManagedServices-EnableCloudFrontDistributionLogging La journalisation est activée pour les CloudFront distributions Amazon.	• BucketName: nom du compartiment Amazon S3 dans lequel vous souhaitez stocker les journaux d'accès. • S3 KeyPrefix : préfixe de l'emplacement dans le compartiment S3 pour les journaux de CloudFront distribution Amazon. • IncludeCookies: indique s'il faut inclure les cookies dans les journaux d'accès. Pour activer la correction automatique, les paramètres préconfigurés suivants doivent être fournis : • BucketName • S3KeyPrefix • IncludeCookies Pour connaître ces contraintes de correction, voir Comment activer la journalisation pour ma CloudFront distribution ?

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G109 - la validation du fichier CloudTrail journal doit être activée AWS Security Hub Chèque correspondant : CloudTrail4.	AWSManagedServices-TrustedRemediatorEnableCloudTrailLogValidation Active la validation CloudTrail du journal de suivi.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
Hs4Ma3G108 - les CloudTrail sentiers doivent être intégrés à Amazon Logs CloudWatch AWS Security Hub Chèque correspondant : CloudTrail5.	AWSManagedServices-IntegrateCloudTrailWithCloudWatch AWS CloudTrail est intégré à CloudWatch Logs.	• CloudWatchLogsLogGroupName: nom du groupe de CloudWatch journaux auquel CloudTrail les journaux sont envoyés. Vous devez utiliser un groupe de journaux qui existe dans votre compte. • CloudWatchLogsRoleName: nom du rôle IAM que le point de terminaison CloudWatch Logs doit assumer pour écrire dans le groupe de journaux d'un utilisateur. Vous devez utiliser un rôle qui existe dans votre compte. Pour activer la correction automatique, les paramètres préconfigurés suivants doivent être fournis : • CloudWatchLogsLogGroupName • CloudWatchLogsRoleName

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G217 - les environnements de CodeBuild projet doivent avoir une configuration de journalisation AWS AWS Security Hub Chèque correspondant : CodeBuild4.	AWSManagedServices-TrustedRemediatorEnableCodeBuildLoggingConfig Active la journalisation du CodeBuild projet.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
Hs4Ma3G306 - La protection contre la suppression des clusters de base de données Neptune doit être activée AWS Security Hub Vérification correspondante : DocumentDB.3	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnDocumentDBSnapshot Supprime l'accès public à l'instantané manuel du cluster Amazon DocumentDB.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G308 - La protection contre la suppression des clusters Amazon DocumentDB doit être activée AWS Security Hub Vérification correspondante : DocumentDB.5	AWSManagedServices-TrustedRemediatorEnableDocumentDBClusterDeletionProtection Active la protection contre les suppressions pour le cluster Amazon DocumentDB.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
Hs4Ma3G323 - La protection contre la suppression des tables DynamoDB doit être activée AWS Security Hub Vérification correspondante : DynamoDB.6	AWSManagedServices-TrustedRemediatorEnableDynamoDBTableDeletionProtection Active la protection contre la suppression pour les tables DynamoDB autres qu'AMS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
EPS02JT06W - Instantanés publics d'Amazon EBS	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnEBSSnapshot L'accès public aux instantanés Amazon EBS est désactivé.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G118 - Les groupes de sécurité VPC par défaut ne doivent pas autoriser le trafic entrant ou sortant AWS Security Hub Contrôle correspondant : EC22.	AWSManagedServices-TrustedRemediatorRemoveAllRulesFromDefaultSG Toutes les règles d'entrée et de sortie du groupe de sécurité par défaut sont supprimées.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
Hs4Ma3G117 - Les volumes EBS attachés doivent être chiffrés au repos AWS Security Hub Contrôle correspondant : EC23.	AWSManagedServices-EncryptInstanceVolume Le volume Amazon EBS joint à l'instance est chiffré.	• KMSKeyId : ID de AWS KMS clé ou ARN pour chiffrer le volume. • DeleteStaleNonEncryptedSnapshotBackups: indicateur qui détermine si la sauvegarde instantanée des anciens volumes non chiffrés doit être supprimée. L'instance est redémarrée dans le cadre de la correction et la restauration est possible si elle `DeleteStaleNonEncryptedSnapshotBackups` est définie sur `false` ce qui facilite la restauration.

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G120 - Les EC2 instances arrêtées doivent être supprimées après une période spécifiée AWS Security Hub Chèque correspondant : EC24.	AWSManagedServices-TerminateInstance(document SSM par défaut pour les modes d'exécution automatique et manuel) EC2 Les instances Amazon arrêtées pendant 30 jours sont résiliées.	Créer une AMIBefore résiliation :. Pour créer l'AMI d'instance en tant que sauvegarde avant de mettre fin à l' EC2 instance, choisissez`true`. Pour ne pas créer de sauvegarde avant de terminer, choisissez`false`. L'argument par défaut est `true`. Aucune contrainte
Hs4Ma3G120 - Les EC2 instances arrêtées doivent être supprimées après une période spécifiée AWS Security Hub Chèque correspondant : EC24.	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime - EC2 Les instances Amazon arrêtées pendant le nombre de jours défini dans Security Hub (la valeur par défaut est 30) sont résiliées.	Créer une AMIBefore résiliation : pour créer l'AMI de l'instance en tant que sauvegarde avant de mettre fin à l' EC2 instance, choisissez`true`. Pour ne pas créer de sauvegarde avant de terminer, choisissez`false`. L'argument par défaut est `true`. Aucune contrainte
Hs4Ma3G121 - Le cryptage par défaut EBS doit être activé AWS Security Hub Contrôle correspondant : 7 EC2.	AWSManagedServices-EncryptEBSByDefault Le chiffrement Amazon EBS est activé par défaut pour Région AWS	Aucun paramètre préconfiguré n'est autorisé. Le chiffrement par défaut est un paramètre spécifique à une région. Si vous l'activez pour une région, vous ne pouvez pas le désactiver pour des volumes ou des instantanés individuels de cette région.

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G124 - Les instances EC2 Amazon doivent utiliser le service de métadonnées d'instance version 2 () IMDSv2 AWS Security Hub Contrôle correspondant : 8 EC2.	AWSManagedServices-TrustedRemediatorActiver l'EC2instance IMDSv2 EC2 Les instances Amazon utilisent le service de métadonnées d'instance version 2 (IMDSv2).	• IMDSv1MetricCheckPeriod: le nombre de jours (42-455) pendant lesquels analyser les statistiques IMDSv1 d'utilisation dans CloudWatch. Si l' EC2 instance Amazon a été créée dans le délai spécifié, l'analyse commence à la date de création de l'instance. • HttpPutResponseHopLimit: nombre maximal de sauts réseau autorisés pour le jeton de métadonnées de l'instance. Cette valeur peut être configurée entre 1 et 2 sauts. Une limite de 1 sauts restreint l'accès par jeton aux processus exécutés directement sur l'instance, tandis qu'une limite de sauts 2 autorise l'accès à partir de conteneurs exécutés sur l'instance. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G207 - les EC2 sous-réseaux ne doivent pas attribuer automatiquement des adresses IP publiques AWS Security Hub Chèque correspondant : EC2.15	AWSManagedServices-UpdateAutoAssignPublicIpv4 Adresses Les sous-réseaux VPC sont configurés pour ne pas attribuer automatiquement d'adresses IP publiques.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
Hs4Ma3G209 - Les listes de contrôle d'accès réseau non utilisées sont supprimées AWS Security Hub Contrôle correspondant : EC2.16	AWSManagedServices-DeleteUnusedNACL Supprimer les ACL réseau inutilisées	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G215 - Les groupes de sécurité EC2 Amazon inutilisés doivent être supprimés AWS Security Hub Chèque correspondant : EC2.22	AWSManagedServices-DeleteSecurityGroups Supprimez les groupes de sécurité inutilisés.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
Hs4Ma3G247 - Amazon Transit EC2 Gateway ne doit pas accepter automatiquement les demandes de pièces jointes VPC AWS Security Hub Chèque correspondant : EC2.23	AWSManagedServices-TrustedRemediatorDisableTGWAutoVPCAttach- Désactive l'acceptation automatique des demandes de pièces jointes VPC pour l'Amazon Transit EC2 Gateway non AMS spécifié.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G235 - L'immuabilité des balises doit être configurée dans les référentiels privés ECR AWS Security Hub Contrôle correspondant : ECR.2	AWSManagedServices-TrustedRemediatorSetImageTagImmutability Définit les paramètres de mutabilité des balises d'image sur IMMUTABLE pour le référentiel spécifié.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
Hs4Ma3G216 - Les référentiels ECR doivent avoir au moins une politique de cycle de vie configurée AWS Security Hub Contrôle correspondant : ECR.3	AWSManagedServices-PutECRRepositoryLifecyclePolicy Le référentiel ECR possède une politique de cycle de vie configurée.	LifecyclePolicyText: le texte de politique du référentiel JSON à appliquer au référentiel. Pour activer la correction automatique, les paramètres préconfigurés suivants doivent être fournis : LifecyclePolicyText
Hs4Ma3G325 - La journalisation des audits doit être activée sur les clusters EKS AWS Security Hub Chèque correspondant : EKS.8	AWSManagedServices-TrustedRemediatorEnableEKSAuditLog Le journal d'audit est activé pour le cluster EKS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G183 - L'équilibreur de charge d'application doit être configuré pour supprimer les en-têtes HTTP AWS Security Hub Contrôle correspondant : ELB.4	AWSConfigRemediation-DropInvalidHeadersForALB Application Load Balancer est configuré avec des champs d'en-tête non valides.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G184 - La journalisation des équilibreurs de charge d'application et des équilibreurs de charge classiques doit être activée AWS Security Hub Contrôle correspondant : ELB.5	AWSManagedServices-EnableELBLogging (document SSM par défaut pour les modes d'exécution automatique et manuel) La journalisation entre Application Load Balancer et Classic Load Balancer est activée.	• BucketName: le nom du compartiment (et non l'ARN). Assurez-vous que la politique de compartiment est correctement configurée pour la journalisation. • S3 KeyPrefix : préfixe de l'emplacement dans le compartiment Amazon S3 pour les journaux Elastic Load Balancing. Pour activer la correction automatique, les paramètres préconfigurés suivants doivent être fournis : • BucketName • S3KeyPrefix Le bucket Amazon S3 doit avoir une politique de bucket qui accorde à Elastic Load Balancing l'autorisation d'écrire les journaux d'accès dans le bucket.

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfig urés pris en charge
Hs4Ma3G184 - La journalisation des équilibre urs de charge d'application et des équilibre urs de charge classiques doit être activée AWS Security Hub Contrôle correspondant : ELB.5	AWSManagedServices-EnableEL BLoggingV2 La journalisation entre Applicati on Load Balancer et Classic Load Balancer est activée.	• TargetBucketTagKey: nom du tag (distinguant majuscules et minuscules) utilisé pour identifie r le compartiment Amazon S3 cible. Utilisez-le avec `TargetBuc ketTagValue` pour étiqueter le compartiment qui servira de compartiment de destination pour la journalisation des accès. • TargetBucketTagValue: valeur de balise (distinguant majuscules et minuscules) utilisée pour identifie r le compartiment Amazon S3 cible. Utilisez-le avec `TargetBuc ketTagKey` pour étiqueter le compartiment qui servira de compartiment de destination pour la journalisation des accès. • S3 BucketPrefix : préfixe (hiérarch ie logique) du compartiment Amazon S3. Le préfixe que vous spécifiez ne doit pas inclure la chaîne `AWSLogs`. Pour plus d'informations, consultez Organisat ion des objets à l'aide de préfixes. Pour activer la correction automatique, les paramètres préconfigurés suivants doivent être fournis : • TargetBucketTagKey • TargetBucketTagValue • S3BucketPrefix

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
		Le bucket Amazon S3 doit avoir une politique de bucket qui accorde à Elastic Load Balancing l'autorisation d'écrire les journaux d'accès dans le bucket.
Hs4Ma3G326 - Le paramètre de blocage de l'accès public à Amazon EMR doit être activé AWS Security Hub Chèque correspondant : EMR.2	AWSManagedServices-TrustedRemediatorEnableEMRBlockPublicAccess Les paramètres de blocage de l'accès public à Amazon EMR sont activés pour le compte.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
Hs4Ma3G135 - les AWS KMS clés ne doivent pas être supprimées par inadvertance AWS Security Hub Contrôle correspondant : KMS.3	AWSManagedServices-CancelKeyDeletion AWS KMS la suppression de la clé est annulée.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G299 - Les instantanés de cluster manuels Amazon DocumentDB ne doivent pas être publics AWS Security Hub Chèque correspondant : Neptune.4	AWSManagedServices-TrustedRemediatorEnableNeptuneDBClusterDeletionProtection Active la protection contre les suppressions pour le cluster Amazon Neptune.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
Hs4Ma3G319 - La protection contre les suppressions doit être activée sur les pare-feux Network Firewall AWS Security Hub Chèque correspondant : 9 NetworkFirewall.	AWSManagedServices-TrustedRemediatorEnableNetworkFirewallDeletionProtection- Active la protection contre la suppression pour AWS Network Firewall.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G223 - les OpenSearch domaines doivent crypter les données envoyées entre les nœuds AWS Security Hub Contrôle correspondant : OpenSearch3.	AWSManagedServices-EnableOpenSearchNodeToNodeEncryption Le chiffrement nœud à nœud est activé pour le domaine.	Aucun paramètre préconfiguré n'est autorisé. Une fois node-to-node le chiffrement activé, vous ne pouvez pas désactiver le paramètre. Prenez plutôt un instantané manuel du domaine chiffré, créez un autre domaine, migrez vos données, puis supprimez l'ancien domaine.
Hs4Ma3G222 - la journalisation des erreurs de OpenSearch domaine dans Logs doit être activée CloudWatch AWS Security Hub Contrôle correspondant : Opensearch.4	AWSManagedServices-EnableOpenSearchLogging La journalisation des erreurs est activée pour le OpenSearch domaine.	CloudWatchLogGroupArn: ARN d'un groupe de CloudWatch journaux Amazon Logs. Pour activer la correction automatique, le paramètre préconfiguré suivant doit être fourni :. CloudWatchLogGroupArn La politique de CloudWatch ressources Amazon doit être configurée avec des autorisations. Pour plus d'informations, consultez la section Activation des journaux d'audit dans le guide de l'utilisateur d'Amazon OpenSearch Service

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G221 - la journalisation des audits doit être activée sur OpenSearch les domaines AWS Security Hub Contrôle correspondant : Opensearch.5	AWSManagedServices-EnableOpenSearchLogging OpenSearch les domaines sont configurés avec la journalisation des audits activée.	CloudWatchLogGroupArn: ARN du groupe CloudWatch Logs dans lequel publier les logs. Pour activer la correction automatique, le paramètre préconfiguré suivant doit être fourni : CloudWatchLogGroupArn La politique de CloudWatch ressources Amazon doit être configurée avec des autorisations. Pour plus d'informations, consultez la section Activation des journaux d'audit dans le guide de l'utilisateur d'Amazon OpenSearch Service
Hs4Ma3G220 - Les connexions aux OpenSearch domaines doivent être cryptées à l'aide du protocole TLS 1.2 AWS Security Hub Contrôle correspondant : Opensearch.8	AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2 La politique TLS est définie sur « Policy-min-TLS-1-2-2019-07` et seules les connexions cryptées via HTTPS (TLS) sont autorisées.	Aucun paramètre préconfiguré n'est autorisé. Les connexions aux OpenSearch domaines sont requises pour utiliser le protocole TLS 1.2. Le chiffrement des données en transit peut affecter les performances. Testez vos applications avec cette fonctionnalité pour comprendre le profil de performance et l'impact du protocole TLS.

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G194 - L'instantané Amazon RDS doit être privé AWS Security Hub Contrôle correspondant : RDS.1	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 L'accès public aux instantanés Amazon RDS est désactivé.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
Hs4Ma3G192 - Les instances de base de données RDS doivent interdire l'accès public, tel que déterminé par la configuration PubliclyAccessible AWS AWS Security Hub Contrôle correspondant : RDS.2	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnRDSInstance Désactivez l'accès public sur l'instance de base de données RDS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfig urés pris en charge
Hs4Ma3G189 - Une surveillance améliorée est configurée pour les instances de base de données Amazon RDS AWS Security Hub Contrôle correspondant : RDS.6	AWSManagedServices-TrustedR emediatorEnableRDSEnhancedM onitoring Activez une surveillance améliorée pour les instances de base de données Amazon RDS	• MonitoringInterval: intervalle, en secondes, entre les points où les métriques de surveillance améliorée sont collectées pour l'instance de base de données. Les intervalles valides sont 0, 1, 5, 10, 15, 30 et 60. Pour désactiver la collecte des métriques de surveilla nce améliorée, spécifiez 0. • MonitoringRoleName: nom du rôle IAM qui permet à Amazon RDS d'envoyer des métriques de surveillance améliorées à Amazon CloudWatch Logs. Si aucun rôle n'est spécifié, le rôle par défaut `rds-monitoring-role` est utilisé ou créé, s'il n'existe pas. Si la surveillance améliorée est activée avant l'exécution de l'automat isation, les paramètres peuvent être remplacés par cette automatisation par les MonitoringRoleName valeurs MonitoringInterval et configurées dans les paramètres préconfigurés.

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G190 - La protection contre la suppression des clusters Amazon RDS doit être activée AWS Security Hub Contrôle correspondant : RDS.7	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection La protection contre la suppression est activée pour les clusters Amazon RDS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
Hs4Ma3G198 - La protection contre la suppression des instances de base de données Amazon RDS doit être activée AWS Security Hub Contrôle correspondant : RDS.8	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection La protection contre la suppression est activée pour les instances Amazon RDS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G199 - Les instances de base de données RDS doivent publier des journaux dans Logs CloudWatch AWS Security Hub Contrôle correspondant : RDS.9	AWSManagedServices-TrustedRemediatorEnableRDSLogExports Les exportations de journaux RDS sont activées pour l'instance de base de données RDS ou le cluster de base de données RDS.	Aucun paramètre préconfiguré n'est autorisé. Le rôle AWSServiceRoleForRDS lié à un service est requis.
Hs4Ma3G160 - L'authentification IAM doit être configurée pour les instances RDS AWS Security Hub Contrôle correspondant : RDS.10	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication AWS Identity and Access Management l'authentification est activée pour l'instance RDS.	ApplyImmediately: indique si les modifications de cette demande et les modifications en attente sont appliquées de manière asynchrone dès que possible. Pour appliquer la modification immédiatement, choisissez. `true` Pour planifier le changement pour la prochaine fenêtre de maintenance, choisisse `zfalse`. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G161 - L'authentification IAM doit être configurée pour les clusters RDS AWS Security Hub Contrôle correspondant : RDS.12	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication L'authentification IAM est activée pour le cluster RDS.	ApplyImmediately: indique si les modifications de cette demande et les modifications en attente sont appliquées de manière asynchrone dès que possible. Pour appliquer la modification immédiatement, choisissez. `true` Pour planifier le changement pour la prochaine fenêtre de maintenance, choisisse `zfalse`. Aucune contrainte
Hs4Ma3G162 - Les mises à niveau automatiques des versions mineures de RDS devraient être activées AWS Security Hub Contrôle correspondant : RDS.13	AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade La configuration automatique de mise à niveau des versions mineures pour Amazon RDS est activée.	Aucun paramètre préconfiguré n'est autorisé. L'instance Amazon RDS doit être en bon `available` état pour que cette correction ait lieu.

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G163 - Les clusters de base de données RDS doivent être configurés pour copier des balises dans des instantanés AWS Security Hub Contrôle correspondant : RDS.16	AWSManagedServices-UpdateRDSCopyTagsToSnapshots `CopyTagtosnapshot` le paramètre pour les clusters Amazon RDS est activé.	Aucun paramètre préconfiguré n'est autorisé. Les instances Amazon RDS doivent être disponibles pour que cette correction ait lieu.
Hs4Ma3G164 - Les instances de base de données RDS doivent être configurées pour copier des balises dans des instantanés AWS Security Hub Contrôle correspondant : RDS.17	AWSManagedServices-UpdateRDSCopyTagsToSnapshots `CopyTagsToSnapshot` le paramètre pour Amazon RDS est activé.	Aucun paramètre préconfiguré n'est autorisé. Les instances Amazon RDS doivent être disponibles pour que cette correction ait lieu.
RSS 93 HQwa1 Instantanés publics Amazon RDS	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 L'accès public aux instantanés Amazon RDS est désactivé.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G103 - Les clusters Amazon Redshift devraient interdire l'accès public AWS Security Hub Contrôle correspondant : Redshift.1	AWSManagedServices-DisablePublicAccessOnRedshiftCluster L'accès public au cluster Amazon Redshift est désactivé.	Aucun paramètre préconfiguré n'est autorisé. La désactivation de l'accès public bloque tous les clients provenant d'Internet. Et le cluster Amazon Redshift est en état de modification pendant quelques minutes pendant que la correction désactive l'accès public au cluster.
Hs4Ma3G106 - La journalisation des audits doit être activée sur les clusters Amazon Redshift AWS Security Hub Contrôle correspondant : Redshift.4	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterAuditLogging La journalisation des audits est activée sur votre cluster Amazon Redshift pendant la période de maintenance.	Aucun paramètre préconfiguré n'est autorisé. Pour activer la correction automatique, les paramètres préconfigurés suivants doivent être fournis. BucketName: Le compartiment doit se trouver dans le même compartiment Région AWS. Le cluster doit disposer des autorisations Read Bucket et Put Object. Si la journalisation du cluster Redshift est activée avant l'exécution de l'automatisation, les paramètres de journalisation peuvent être remplacés par cette automatisation par les `S3KeyPrefix` valeurs `BucketName` et configurées dans les paramètres préconfigurés.

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G105 - Amazon Redshift devrait activer les mises à niveau automatiques vers les versions majeures AWS Security Hub Contrôle correspondant : Redshift.6	AWSManagedServices-EnableRedshiftClusterVersionAutoUpgrade- Les mises à niveau des versions majeures sont appliquées automatiquement au cluster pendant la période de maintenance. Il n'y a pas de temps d'arrêt immédiat pour le cluster Amazon Redshift, mais votre cluster Amazon Redshift peut subir une interruption de service pendant sa période de maintenance s'il est mis à niveau vers une version majeure.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
Hs4Ma3G104 - Les clusters Amazon Redshift doivent utiliser un routage VPC amélioré AWS Security Hub Contrôle correspondant : Redshift.7	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterEnhancedVPCRouting Le routage VPC amélioré est activé pour les clusters Amazon Redshift.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G173 - Le paramètre S3 Block Public Access doit être activé au niveau du bucket AWS Security Hub Contrôle correspondant : S3.8	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess Les blocs d'accès public au niveau du compartiment sont appliqués au compartiment Amazon S3.	Aucun paramètre préconfiguré n'est autorisé. Cette correction peut affecter la disponibilité des objets S3. Pour plus d'informations sur la manière dont Amazon S3 évalue l'accès, consultez Blocage de l'accès public à votre espace de stockage Amazon S3.

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfig urés pris en charge
Hs4Ma3G230 - La journalis ation des accès au serveur de compartiment S3 doit être activée AWS Security Hub Contrôle correspondant : S3.9	AWSManagedServices-EnableBu cketAccessLogging(document SSM par défaut pour les modes d'exécuti on automatique et manuel) La journalisation des accès au serveur Amazon S3 est activée.	• TargetBucket: nom du compartim ent S3 pour stocker les journaux d'accès au serveur. • TargetObjectKeyFormat: format de clé Amazon S3 pour les objets du journal (les valeurs distingue nt les majuscules et minuscules). Pour utiliser le format simple des clés S3 pour les objets du journal, choisissez`SimplePrefix` . Pour utiliser la clé S3 partition née pour les objets du journal et EventTime pour le préfixe partition né, choisissez. `Partition edPrefixEventTime` Pour utiliser la clé S3 partitionnée pour les objets du journal et DeliveryT ime pour le préfixe partition né, choisissez. `Partition edPrefixDeliveryTime` Les valeurs valides sont `SimplePre fix` , `PartitionedPrefixE ventTime` et `Partition edPrefixDeliveryTime` . Pour activer la correction automatiq ue, le paramètre préconfiguré suivant doit être fourni :. TargetBucket Le compartiment de destination doit se trouver dans le même Région AWS compartiment Compte AWS que le compartiment source, avec

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
		les autorisations appropriées pour la livraison des journaux. Pour plus d'informations, consultez Activer la journalisation des accès au serveur Amazon S3.

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfig urés pris en charge
Hs4Ma3G230 — La journalis ation des accès au serveur de compartiments S3 doit être activée AWS Security Hub Contrôle correspondant : S3.9	AWSManagedServices-TrustedR emediatorEnableBucketAccess LoggingV2 - La journalisation des compartiments Amazon S3 est activée.	• TargetBucketTagKey: nom du tag (distinguant majuscules et minuscules) permettant d'identif ier le compartiment cible. Utilisez-le et TargetBucketTagValuepour étiqueter le compartiment à utiliser comme compartiment de destinati on pour la journalisation des accès. • TargetBucketTagValue: valeur de balise (sensible aux majuscules et minuscules) pour identifier le compartiment cible, utilisez-la et TargetBucketTagKeypour étiqueter le compartiment à utiliser comme compartiment de destination pour la journalisation des accès. • TargetObjectKeyFormat: format de clé Amazon S3 pour les objets de journal (les valeurs distingue nt majuscules et minuscules) : Pour utiliser le format simple des clés S3 pour les objets de journal, choisissez SimplePrefix. Pour utiliser la clé S3 partition née pour les objets du journal et EventTime pour le préfixe partition né, choisissez. PartitionedPrefixE ventTime Pour utiliser la clé S3 partitionnée pour les objets du journal et DeliveryTime pour le préfixe partitionné, choisissez. PartitionedPrefixDeliveryTime

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
		La valeur par défaut est PartitionedPrefixEventTime. Pour activer la correction automatique, les paramètres suivants doivent être fournis : TargetBucketTagKeyet TargetBucketTagValue. Le compartiment de destination doit se trouver dans le même Région AWS compartiment Compte AWS que le compartiment source, avec les autorisations appropriées pour la livraison des journaux. Pour plus d'informations, consultez Activer la journalisation des accès au serveur Amazon S3.
Pfx 0 RwqBli Autorisations pour le compartiment Amazon S3	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess Blocage de l'accès public	Aucun paramètre préconfiguré n'est autorisé. Cette vérification repose sur plusieurs critères d'alerte. Cette automatisation permet de résoudre les problèmes d'accès public. La correction des autres problèmes de configuration signalés par Trusted Advisor n'est pas prise en charge. Cette correction prend en charge la correction des compartiments S3 Service AWS créés (par exemple, cf-templates-000000000000).

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G272 - Les utilisateurs ne doivent pas avoir d'accès root aux instances de bloc-notes SageMaker AWS Security Hub Contrôle correspondant : SageMaker3.	AWSManagedServices-TrustedRemediatorDisableSageMakerNotebookInstanceRootAccess L'accès root pour les utilisateurs est désactivé pour les instances de SageMaker bloc-notes.	Aucun paramètre préconfiguré n'est autorisé. Cette correction entraîne une panne si l'instance du SageMaker bloc-notes est dans InService cet état.
Hs4Ma3G179 - Les sujets SNS doivent être chiffrés au repos en utilisant AWS KMS AWS Security Hub Contrôle correspondant : SNS.1	AWSManagedServices-EnableSNSEncryptionAtRest La rubrique SNS est configurée avec le chiffrement côté serveur.	KmsKeyId: ID d'une clé principale client (CMK) AWS gérée pour Amazon SNS ou d'une clé CMK personnalisée à utiliser pour le chiffrement côté serveur (SSE). La valeur par défaut est définie sur `alias/aws/sns` . Si une AWS KMS clé personnalisée est utilisée, elle doit être configurée avec les autorisations appropriées. Pour plus d'informations, consultez Activer le chiffrement côté serveur (SSE) pour une rubrique Amazon SNS

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Hs4Ma3G158 - Les documents SSM ne doivent pas être publics AWS Security Hub Contrôle correspondant : SSM.4	AWSManagedServices-TrustedRemediatorDisableSSMDocPublicSharing- Désactive le partage public du document SSM.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfig urés pris en charge
Hs4Ma3G13 6 - Les files d'attente Amazon SQS doivent être chiffrées au repos AWS Security Hub Chèque correspondant : SQS.1	AWSManagedServices-EnableSQ SEncryptionAtRest Les messages dans Amazon SQS sont chiffrés.	• SqsManagedSseEnabled: défini sur `true` pour activer le chiffreme nt des files d'attente côté serveur à l'aide des clés de chiffrement détenues par Amazon SQS, défini sur pour activer le chiffrement des files d'attente côté serveur `false` à l'aide d'une clé. AWS KMS • KMSKeyID : ID ou alias d'une clé principale client (CMK) AWS gérée pour Amazon SQS ou d'une clé CMK personnalisée à utiliser pour le chiffrement côté serveur de la file d'attente. S'il n'est pas fourni, alias/aws/sqs est utilisé. • KmsDataKeyReusePeriodSecond s: durée, en secondes, pendant laquelle Amazon SQS peut réutiliser une clé de données pour chiffrer ou déchiffrer des messages avant de réappeler. AWS KMS Entier en secondes, compris entre 60 secondes (1 minute) et 86 400 secondes (24 heures). Ce paramètre est ignoré s'il `SqsManagedSseEnabled` est défini sur`true`. ReceiveMessage Les demandes anonymes SendMessage et envoyées à la file d'attente cryptée sont rejetées. Toutes les demandes adressées aux files d'attente

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
		avec le chiffrement SSE activé doivent utiliser HTTPS et Signature version 4.

Trusted Advisor contrôles de tolérance aux pannes pris en charge par Trusted Remediator

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
c18d2gz138 Récupération d'Amazon DynamoDB Point-in-time	AWSManagedServices-TrustedRemediatorEnableDDBPITR Permet point-in-time la restauration des tables DynamoDB.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
R365S2QDDF Amazon S3 Bucket Versioning	AWSManagedServices-TrustedRemediatorEnableBucketVersioning La gestion des versions des compartiments Amazon S3 est activée.	Aucun paramètre préconfiguré n'est autorisé. Cette correction ne prend pas en charge la correction des compartiments S3 Service AWS créés (par exemple cf-templates-00000 0000000).
BueAdJ7NRP Journalisation des compartiments Amazon S3	AWSManagedServices-EnableBucketAccessLogging La journalisation des compartiments Amazon S3 est activée.	• TargetBucket: nom du compartiment S3 pour stocker les journaux d'accès au serveur. • TargetObjectKeyFormat: format de clé Amazon S3 pour les objets de journal. Pour utiliser le format simple des clés S3 pour les objets de journal, choisissez`SimplePre`

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
		`fix` . Pour utiliser la clé S3 partitionnée pour les objets du journal et EventTime pour le préfixe partitionné, choisissez. `PartitionedPrefixEventTime` Pour utiliser la clé S3 partitionnée pour les objets du journal et DeliveryTime pour le préfixe partitionné, choisissez. `PartitionedPrefixDeliveryTime` L'argument par défaut est `PartitionedPrefixEventTime` . Les valeurs valides sont`SimplePrefix` , `PartitionedPrefixEventTime` et `PartitionedPrefixDeliveryTime` (distinguez majuscules et minuscules). Pour activer la correction automatique, les paramètres préconfigurés suivants doivent être fournis : • TargetBucket Le compartiment de destination doit se trouver dans le même Région AWS compartiment Compte AWS que le compartiment source, avec les autorisations appropriées pour la livraison des journaux. Pour plus d'informations, consultez Activer la

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
		journalisation des accès au serveur Amazon S3.
F2iK5R6DEP Amazon RDS Multi-AZ	AWSManagedServices-TrustedRemediatorEnableRDSMultiAZ Le déploiement de zones de disponibilité multiple est activé.	Aucun paramètre préconfiguré n'est autorisé. Une dégradation des performances est possible lors de cette modification.
H7 IgTzj TYb Instantanés Amazon EBS	AWSManagedServices-TrustedRemediatorCreateEBSSnapshot Amazon EBSsnapshots est créé.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
en QPADk ZVH Sauvegardes RDS	AWSManagedServices-EnableRDSBackupRetention La conservation des sauvegardes Amazon RDS est activée pour la base de données.	• BackupRetentionPeriod: le nombre de jours (1 à 35) pendant lesquels les sauvegardes automatisées sont conservées. • ApplyImmediately: indique si le changement de rétention des sauvegardes RDS et les modifications en attente sont appliquées de manière asynchrone dès que possible. Choisissez `true` d'appliquer la modification immédiatement ou `false` de la planifier pour la fenêtre de maintenance suivante. Si le `ApplyImmediately` paramètre est défini sur`true`, les modifications en attente sur la base de données sont appliquées avec le paramètre de RDSBackup rétention.

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfig urés pris en charge
c1qf5bt013 La mise à l'échelle automatique du stockage est désactivée sur les instances de base de données Amazon RDS	AWSManagedServices-TrustedR emediatorEnableRDSInstanceS torageAutoScaling- Le dimension nement automatique du stockage est activé pour l'instance de base de données Amazon RDS.	• MaxAllocatedStorageIncrease Percentage: Le pourcentage d'augmentation du courant AllocatedStorage, pour définir le MaxAllocatedStorage. La valeur par défaut est définie sur 26. Vous devez définir le seuil de stockage maximal à au moins 10 % de plus que le stockage actuellement alloué. Il est recommandé de fixer le seuil de stockage maximal à au moins 26 % de plus. Pour plus de détails, consultez la section Gestion automatique de la capacité avec le dimensionnement automatique du stockage Amazon Relational Database Service. Aucune contrainte
7q GXs KlUw Vidange de la connexion Classic Load Balancer	AWSManagedServices-TrustedR emediatorEnableCLBConnectio nDraining Le drainage des connexions est activé pour Classic Load Balancer.	ConnectionDrainingTimeout: durée maximale, en secondes, pendant laquelle les connexions existantes restent ouvertes avant de désenregi strer les instances. La valeur par défaut est définie sur les 300 secondes. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfig urés pris en charge
c18d2gz107 Amazon EBS n'est pas inclus dans le forfait AWS Backup	AWSManagedServices-TrustedRemediatorAddVolumeToBackupPlan Amazon EBS est inclus dans le AWS Backup plan.	La correction balise le volume Amazon EBS avec la paire de balises suivante. La paire de balises doit correspondre aux critères de sélection des ressources basés sur les balises pour AWS Backup. • TagKey • TagValue Aucune contrainte
c18d2gz107 La table Amazon DynamoDB n'est pas incluse dans le forfait AWS Backup	AWSManagedServices-TrustedRemediatorAddDynamoDBToBackupPlan La table Amazon DynamoDB est incluse dans le plan. AWS Backup	La correction balise Amazon DynamoDB avec la paire de balises suivante. La paire de balises doit correspondre aux critères de sélection des ressources basés sur les balises pour AWS Backup. • TagKey • TagValue Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
c18d2gz117 Amazon EFS n'est pas inclus dans le AWS Backup forfait	AWSManagedServices-TrustedRemediatorAddEFSToBackupPlan Amazon EFS est inclus dans le AWS Backup forfait.	La correction balise Amazon EFS avec la paire de balises suivante. La paire de balises doit correspondre aux critères de sélection des ressources basés sur les balises pour AWS Backup. • TagKey • TagValue Aucune contrainte
c18d2gz105 Équilibrage de charge entre zones sur les Network Load Balancers	AWSManagedServices-TrustedRemediatorEnableNLBCrossZoneLoadBalancing L'équilibrage de charge entre zones est activé sur Network Load Balancer.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
c1qf5bt026 Le `synchronous_commit` paramètre Amazon RDS est désactivé	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Le paramètre `synchronous_commit` est activé pour Amazon RDS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
c1qf5bt030 Le `innodb_flush_log_at_trx_commit` paramètre Amazon RDS n'est pas 1	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Le paramètre `innodb_flush_log_at_trx_commit` est défini sur 1 pour Amazon RDS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
c1qf5bt031 Le `sync_binlog` paramètre Amazon RDS est désactivé	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Le paramètre `sync_binlog` est activé pour Amazon RDS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
c1qf5bt036 Le réglage des `innodb_default_row_format` paramètres Amazon RDS n'est pas sûr	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Le paramètre `innodb_default_row_format` est défini sur `DYNAMIC` pour Amazon RDS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
c18d2gz145 La surveillance EC2 détaillée d'Amazon n'est pas activée	AWSManagedServices-TrustedRemediatorEnableEC2InstanceDetailedMonitoring La surveillance détaillée est activée pour Amazon EC2.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Trusted Advisor contrôles de performance pris en charge par Trusted Remediator

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfig urés pris en charge
COr6dfpM06 AWS Lambda fonctions sous-provisionnées pour ce qui est de la taille de la mémoire	AWSManagedServices-ResizeLa mbdaMemory La taille de mémoire des fonctions Lambda est redimensionnée selon la taille de mémoire recommandée fournie par. Trusted Advisor	RecommendedMemorySize: allocatio n de mémoire recommandée pour la fonction Lambda. La plage de valeurs est comprise entre 128 et 10240. Si la taille de la fonction Lambda est modifiée avant l'exécution de l'automatisation, cette automatisation peut remplacer les paramètres par la valeur recommandée par. Trusted Advisor
ZRxQlPsb6c EC2 Instances Amazon à haut taux d'utilisation	AWSManagedServices-ResizeIn stanceByOneLevel Les EC2 instances Amazon sont redimensionnées selon un type d'instance supérieur dans le même type de famille d'instances. Les instances sont arrêtées et démarrées pendant l'opération de redimensi onnement et retournent à l'état initial une fois l'exécution terminée. Cette automatisation ne prend pas en charge le redimensionnement des instances qui se trouvent dans un Auto Scaling Group.	• MinimumDaysSinceLastChange: le nombre minimum de jours écoulés depuis le dernier changemen t de type d'instance. Si le type d'instance a été modifié dans le délai spécifié, le type d'instance n'est pas modifié. 0À utiliser pour ignorer cette validation. L'argument par défaut est 7. • Créer un AMIBefore redimensi onnement : pour créer l'AMI de l'instance en tant que sauvegard e avant le redimensionnement, choisissez. `true` Pour ne pas créer de sauvegarde, choisisse `zfalse`. L'argument par défaut est `false`. Les valeurs valides sont `true` et `false` (distinction majuscules et minuscules).

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
		• ResizeIfStopped: Pour procéder au changement de taille de l'instance, même si l'instance est dans un état arrêté, choisissez`true`. Pour ne pas redimensionner automatiquement l'instance en cas d'arrêt, choisissez`false`. Les valeurs valides sont `true` et `false` (distinction majuscules et minuscules). Aucune contrainte
c1qf5bt021 `innodb_change_buffering` Paramètre Amazon RDS utilisant une valeur inférieure à la valeur optimale	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter La valeur du `innodb_change_buffering` paramètre est définie sur `NONE` Amazon RDS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
c1qf5bt025 Le `autovacuum` paramètre Amazon RDS est désactivé	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Le paramètre `autovacuum` est activé pour Amazon RDS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
c1qf5bt028 Le `enable_indexonlyscan` paramètre Amazon RDS est désactivé	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Le paramètre `enable_indexonlyscan` est activé pour Amazon RDS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
c1qf5bt029 Le `enable_indexscan` paramètre Amazon RDS est désactivé	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Le paramètre `enable_indexscan` est activé pour Amazon RDS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
c1qf5bt032 Le `innodb_stats_persistent` paramètre Amazon RDS est désactivé	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Le paramètre `innodb_stats_persistent` est activé pour Amazon RDS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte
c1qf5bt037 Le `general_logging` paramètre Amazon RDS est activé	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Le paramètre `general_logging` est désactivé pour Amazon RDS.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Trusted Advisor vérifications des limites de service prises en charge par Trusted Remediator

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Ln7RR0L7J9 EC2-Adresse IP élastique VPC	AWSManagedServices-UpdateVpcElasticIPQuota Une nouvelle limite pour les adresses IP élastiques EC2 -VPC est demandée. Par défaut, la limite est augmentée de 3.	Incrément : nombre nécessaire pour augmenter le quota actuel. L'argument par défaut est 3. Si cette automatisation est exécutée plusieurs fois avant que le Trusted Advisor contrôle ne soit mis à jour avec le OK statut, il se peut qu'il y ait une augmentation de la limite plus élevée.
Km7QQ0L7J9 Passerelles Internet VPC	AWSManagedServices-IncreaseServiceQuota- Une nouvelle limite pour les passerelles Internet VPC est demandée. Par défaut, la limite est augmentée de trois.	Incrément : nombre nécessaire pour augmenter le quota actuel. L'argument par défaut est 3. Si cette automatisation est exécutée plusieurs fois avant que le Trusted Advisor contrôle ne soit mis à jour avec le OK statut, il se peut qu'il y ait une augmentation de la limite plus élevée.
JL7PP0L7J9 VPC	AWSManagedServices-IncreaseServiceQuota Une nouvelle limite pour le VPC est demandée. Par défaut, la limite est augmentée de 3.	Incrément : nombre nécessaire pour augmenter le quota actuel. L'argument par défaut est 3. Si cette automatisation est exécutée plusieurs fois avant que le Trusted Advisor contrôle ne soit mis à jour avec le OK statut, il se peut qu'il y ait une augmentation de la limite plus élevée.

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
Fw7HH0L7J9 Groupes Auto Scaling	AWSManagedServices-IncreaseServiceQuota Une nouvelle limite pour les groupes Auto Scaling est demandée. Par défaut, la limite est augmentée de 3.	Incrément : nombre nécessaire pour augmenter le quota actuel. L'argument par défaut est 3. Si cette automatisation est exécutée plusieurs fois avant que le Trusted Advisor contrôle ne soit mis à jour avec le OK statut, il se peut qu'il y ait une augmentation de la limite plus élevée.
3 Njm0 DJQO9 Groupes d'options RDS	AWSManagedServices-IncreaseServiceQuota Une nouvelle limite pour les groupes d'options Amazon RDS est demandée. Par défaut, la limite est augmentée de 3.	Incrément : nombre nécessaire pour augmenter le quota actuel. L'argument par défaut est 3. Si cette automatisation est exécutée plusieurs fois avant que le Trusted Advisor contrôle ne soit mis à jour avec le OK statut, il se peut qu'il y ait une augmentation de la limite plus élevée.
EM8b3yLRTr ELB Application Load Balancers	AWSManagedServices-IncreaseServiceQuota Une nouvelle limite pour les équilibreurs de charge d'application ELB est demandée. Par défaut, la limite est augmentée de 3.	Incrément : nombre nécessaire pour augmenter le quota actuel. L'argument par défaut est 3. Si cette automatisation est exécutée plusieurs fois avant que le Trusted Advisor contrôle ne soit mis à jour avec le OK statut, il se peut qu'il y ait une augmentation de la limite plus élevée.

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfig urés pris en charge
8 WiQ K YSt25 Dispositifs d'équilibrage de charge de réseau ELB	AWSManagedServices-Increase ServiceQuota Une nouvelle limite pour les équilibre urs de charge réseau ELB est demandée. Par défaut, la limite est augmentée de 3.	Incrément : nombre nécessaire pour augmenter le quota actuel. L'argument par défaut est 3. Si cette automatisation est exécutée plusieurs fois avant que le Trusted Advisor contrôle ne soit mis à jour avec le 0K statut, il se peut qu'il y ait une augmentation de la limite plus élevée.

Trusted Advisor contrôles d'excellence opérationnelle pris en charge par Trusted Remediator

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfig urés pris en charge
c18d2gz125 Amazon API Gateway ne consigne pas les journaux d'exécution	AWSManagedServices-TrustedR emediatorEnableAPIGateWayEx ecutionLogging La journalisation de l'exécution est activée au stade de l'API.	Aucun paramètre préconfiguré n'est autorisé. Vous devez autoriser API Gateway à lire et à écrire les journaux de votre compte afin CloudWatch d'activer le journal d'exécution. Reportez-vous à la section Configurer la CloudWatch journalisation pour REST APIs dans API Gateway pour plus de détails.
c18d2gz168 La protectio n contre la suppression d'Elastic Load	AWSManagedServices-TrustedR emediatorEnableELBDeletionP rotection- La protection contre la suppression est activée pour Elastic Load Balancer.	Aucun paramètre préconfiguré n'est autorisé. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfig urés pris en charge
Balancing n'est pas activée pour les équilibreurs de charge		
c1qf5bt012 Amazon RDS Performance Insights est désactivé	AWSManagedServices-TrustedR emediatorEnableRDSPerforman ceInsights Performance Insights est activé pour Amazon RDS.	• PerformanceInsightsRetentio nPeriod: le nombre de jours pendant lesquels les données Performance Insights sont conservées. Valeurs valides : 7 ou mois * 31, où le mois est un nombre de mois compris entre 1 et 23. Exemples : 93 (3 mois* 31), 341 (11 mois* 31), 589 (19 mois* 31) ou731. • PerformanceInsightsKMSKeyID : identifiant AWS KMS clé pour le chiffrement des données Performance Insights. Si vous ne spécifiez aucune valeur pour PerformanceInsights KMSKey Id, Amazon RDS utilise votre AWS KMS clé par défaut. Aucune contrainte

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfigurés pris en charge
c1fd6b96l4 Journaux d'accès Amazon S3 activés	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 La journalisation des accès au compartiment Amazon S3 est activée.	• TargetBucketTagValue: valeur de balise (sensible aux majuscules et minuscules) pour identifier le compartiment cible, utilisez-la et TargetBucketTagKey pour étiqueter le compartiment à utiliser comme compartiment de destination pour la journalisation des accès. • TargetObjectKeyFormat: format de clé Amazon S3 pour les objets du journal (les valeurs distinguent les majuscules et minuscules). Pour utiliser le format simple des clés S3 pour les objets du journal, choisissez`SimplePrefix` . Pour utiliser la clé S3 partitionnée pour les objets du journal et EventTime pour le préfixe partitionné, choisissez. `PartitionedPrefixEventTime` Pour utiliser la clé S3 partitionnée pour les objets du journal et DeliveryTime pour le préfixe partitionné, choisissez. `PartitionedPrefixDeliveryTime` Les valeurs valides sont `SimplePrefix` , `PartitionedPrefixEventTime` et `PartitionedPrefixDeliveryTime` . Pour activer la correction automatique, le paramètre préconfiguré suivant

Identifiant et nom du chèque	Nom du document SSM et résultat attendu	Paramètres et contraintes préconfig urés pris en charge
		doit être fourni : TargetBucketTagKey et. TargetBucketTagValue Le compartiment de destination doit se trouver dans le même Région AWS compartiment Compte AWS que le compartiment source, avec les autorisations appropriées pour la livraison des journaux. Pour plus d'informations, consultez Activer la journalisation des accès au serveur Amazon S3.

Configurer Trusted Advisor la correction des chèques dans Trusted Remediator

Les configurations sont stockées dans le AWS AppConfig cadre de l'application Trusted Remediator. Chaque catégorie de Trusted Advisor contrôle possède un profil de configuration distinct. Pour plus d'informations sur les Trusted Advisor catégories, voir Afficher les catégories de vérification.

Vous pouvez configurer les mesures correctives par ressource ou par Trusted Advisor vérification. Vous pouvez appliquer des exceptions à l'aide de balises de ressources.

> **Note**
>
> La correction des Trusted Advisor résultats est actuellement configurée à l'aide de AWS AppConfig, et cette fonctionnalité est entièrement prise en charge aujourd'hui. AMS prévoit que cela changera à l'avenir. Il est recommandé d'éviter de créer des automatisations qui en dépendent AWS AppConfig, car cette méthode est sujette à modification. Sachez que vous devrez peut-être mettre à jour ou modifier les automatisations créées autour de l' AWS AppConfig implémentation actuelle à l'avenir pour des raisons de compatibilité.
> L'indicateur de fonctionnalité Compute Optimizer -> EC2 instances comporte des paramètres supplémentaires :

- allow-upscale Pour autoriser les instances haut de gamme sous-provisionnées et non optimisées. EC2 La valeur définie par défaut est « false ».
- min-savings-opportunity-percentagePourcentage d'économie minimum : possibilité de correction automatisée. La valeur par défaut est de 10 %

Configurations de correction par défaut

Les configurations pour les Trusted Advisor contrôles individuels sont stockées sous forme d' AWS AppConfig indicateurs. Le nom du drapeau correspond au nom du chèque. Chaque configuration de vérification contient les attributs suivants :

- mode d'exécution : Détermine la manière dont Trusted Remediator effectue la correction par défaut :
  - Automatisé : Trusted Remediator corrige automatiquement les ressources en créant un document SSM OpsItem, en exécutant le document, puis en le résolvant une OpsItem fois l'exécution réussie.
  - Manuel : Un OpsItem est créé, mais le document SSM n'est pas exécuté automatiquement. Vous passez en revue et exécutez manuellement le document SSM depuis OpsItem la AWS Systems Manager OpsCenter console.
  - Conditionnel : la correction est désactivée par défaut. Vous pouvez l'activer pour des ressources spécifiques à l'aide de balises. Pour plus d'informations, consultez les sections suivantes Personnalisez la correction à l'aide de balises de ressources etPersonnalisez la correction à l'aide de balises de remplacement des ressources.
  - Inactif : aucune correction n'a lieu et aucune correction n' OpsItem est créée. Vous ne pouvez pas remplacer le mode d'exécution de la Trusted Advisor vérification définie comme inactive.
- paramètres préconfigurés : entrez les valeurs des paramètres du document SSM requis pour la correction automatique, au format, séparées par une virgule (`Parameter=Value`,). Consultez Trusted Advisor contrôles pris en charge par Trusted Remediator les paramètres préconfigurés pris en charge pour le document SSM associé à chaque vérification.
- alternative-automation-document: cet attribut permet de remplacer le document d'automatisation existant par un autre document compatible (si disponible pour la vérification spécifique). Par défaut, cet attribut n'est pas sélectionné.

> **Note**
>
> L'`alternative-automation-document`attribut ne prend pas en charge les documents d'automatisation personnalisés. Vous pouvez utiliser les documents d'automatisation de Trusted Remediator déjà pris en charge répertoriés dansTrusted Advisor contrôles pris en charge par Trusted Remediator.
> Par exemple, pour le contrôle`Qch7DwouX1`, trois documents SSM sont associés : AWSManagedServices-StopEC 2Instance AWSManagedServices-ResizeInstanceByOneLevel, et. AWSManagedServices-TerminateInstance La valeur pour `alternative-automation-document` peut être AWSManagedServices-ResizeInstanceByOneLevel soit AWSManagedServices-TerminateInstance (AWSManagedServices-StopEC2Instance est le document SSM par défaut à corriger`Qch7DwouX1`).

La valeur de chaque attribut doit correspondre aux contraintes de cet attribut.

> **Tip**
>
> Avant d'appliquer les configurations par défaut pour vos Trusted Advisor vérifications, il est recommandé d'envisager d'utiliser les fonctionnalités de balisage des ressources et de remplacement des ressources décrites dans les sections suivantes. Les configurations par défaut s'appliquent à toutes les ressources du compte, ce qui n'est peut-être pas souhaitable dans tous les cas.

Voici un exemple de capture d'écran de console avec le mode d'exécution défini sur Manuel et les attributs correspondant à leurs contraintes.

Personnalisez la correction à l'aide de balises de ressources

Les manual-for-tagged-onlyattributs automated-for-tagged-onlyet de la configuration des vérifications vous permettent de spécifier des balises de ressources indiquant la manière dont vous souhaitez corriger les vérifications individuelles. Il est recommandé d'utiliser cette méthode lorsque vous devez

appliquer un comportement de correction cohérent à un groupe de ressources partageant le même tag ou les mêmes tags. Les descriptions de ces balises sont les suivantes :

- automated-for-tagged-only: Spécifiez des balises de ressources (une ou plusieurs paires de balises, séparées par des virgules) pour que les vérifications soient corrigées automatiquement, quel que soit le mode d'exécution par défaut.
- manual-for-tagged-only: Spécifiez des balises de ressources (une ou plusieurs paires de balises, séparées par des virgules) pour les corrections qui doivent être exécutées manuellement, quel que soit le mode d'exécution par défaut.

Par exemple, si vous souhaitez activer la correction automatique pour toutes les ressources hors production et appliquer la correction manuelle pour les ressources de production, vous pouvez définir votre configuration comme suit :

```
"execution-mode": "Conditional",
"automated-for-tagged-only": "Environment=Non-Production",
"manual-for-tagged-only": "Environment=Production",
```

Une fois les configurations précédentes définies sur vos ressources, vérifiez que le comportement de correction est le suivant :

- Les ressources étiquetées avec « Environment=Non-Production » sont corrigées automatiquement.
- Les ressources étiquetées avec « Environment=Production » nécessitent une intervention manuelle pour être corrigées.
- Les ressources dépourvues de la balise « Environment » suivent le mode d'exécution par défaut (« Conditionnel », dans ce cas). Aucune action n'est donc entreprise sur les ressources restantes).

Pour obtenir une assistance supplémentaire concernant vos configurations, contactez votre architecte cloud.

Personnalisez la correction à l'aide de balises de remplacement des ressources

Les balises Resource Override vous permettent de personnaliser le comportement de correction pour les ressources individuelles, quelles que soient leurs balises. En ajoutant une balise spécifique à une ressource, vous remplacez le mode d'exécution par défaut pour cette ressource et le Trusted Advisor contrôle. La balise de remplacement des ressources a priorité sur la configuration par défaut et les paramètres de balisage des ressources. Ainsi, si vous définissez le mode d'exécution par défaut sur

Automatisé, Manuel ou Conditionnel pour une ressource à l'aide de la balise resource override, il remplace le mode d'exécution par défaut et toutes les configurations de balisage des ressources.

Pour modifier le mode d'exécution d'une ressource, procédez comme suit :

1. Identifiez les ressources pour lesquelles vous souhaitez annuler la configuration de correction.
2. Déterminez le Trusted Advisor numéro du chèque que vous souhaitez annuler. Vous trouverez le check IDs des enregistrements pris Trusted Advisor en chargeTrusted Advisor contrôles pris en charge par Trusted Remediator.
3. Ajoutez une balise aux ressources avec la clé et la valeur suivantes :

   - Clé du tag : `TR-`*`Trusted Advisor check ID`*`-Execution-Mode` (sensible aux majuscules et minuscules)

     Dans l'exemple de clé de balise précédent, `Trusted Advisor check ID` remplacez-le par l'identifiant unique de la Trusted Advisor vérification que vous souhaitez annuler.
   - Valeur de balise : utilisez l'une des valeurs suivantes pour la valeur de balise :
     - Automatisé : Trusted Remediator corrige automatiquement la ressource pour cette Trusted Advisor vérification.
     - Manuel : Un OpsItem est créé pour la ressource, mais la correction n'est pas effectuée automatiquement. Vous passez en revue et exécutez la correction manuellement à partir du OpsItem.
     - Inactif : la correction et OpsItem la création ne sont pas effectuées pour cette ressource et le Trusted Advisor contrôle spécifié.

Par exemple, pour corriger automatiquement un volume Amazon EBS avec l'ID de Trusted Advisor vérification, `DAvU99Dc4C` ajoutez une balise au volume EBS. La clé de balise est `TR-DAvU99Dc4C-Execution-Mode` et la valeur de la balise est`Automated`.

Voici un exemple de console affichant la section Tags :

Flux de décision concernant le mode d'exécution

Il existe plusieurs niveaux pour configurer le mode d'exécution de vos ressources et de chaque Trusted Advisor contrôle. Le schéma suivant montre comment Trusted Remediator décide du mode d'exécution à utiliser en fonction de vos configurations :

Configurer les didacticiels de correction

Les didacticiels suivants fournissent des exemples de création de mesures correctives courantes dans Trusted Remediator.

Corrigez toutes les ressources manuellement

Cet exemple configure la correction manuelle pour tous les volumes Amazon EBS portant l'ID de Trusted Advisor contrôle DAv U99Dc4C (volumes Amazon EBS sous-utilisés).

Configurer la correction manuelle pour les volumes Amazon EBS avec l'ID de contrôle U99Dc4C DAv

1. Ouvrez la AWS AppConfig console sur https://console.aws.amazon.com/systems-manager/appconfig.

   Assurez-vous de vous connecter en tant que compte d'administrateur délégué.
2. Sélectionnez Trusted Remediator dans la liste des applications.
3. Choisissez le profil de configuration d'optimisation des coûts.
4. Sélectionnez l'indicateur Amazon EBS Volumes sous-utilisés.
5. Pour le mode exécution, sélectionnez Manuel.
6. Assurez-vous que les manual-for-tagged-onlyattributs automated-for-tagged-onlyet sont vides. Ces attributs sont utilisés pour remplacer le mode d'exécution par défaut pour les ressources dont les balises correspondent.

   Voici un exemple de section Attributs avec des valeurs vides pour automated-for-tagged-onlyet manual-for-tagged-onlyet Manuel pour le mode exécution :

7. Choisissez Enregistrer pour mettre à jour la valeur, puis sélectionnez Enregistrer la nouvelle version pour appliquer les modifications. Vous devez sélectionner Enregistrer la nouvelle version pour que Trusted Remediator reconnaisse la modification.
8. Assurez-vous que vos volumes Amazon EBS ne comportent pas de balise avec la clé`TR-DAvU99Dc4C-Execution-Mode`. Cette clé de balise remplace le mode d'exécution par défaut pour ce volume EBS.

Corriger automatiquement toutes les ressources, à l'exception des ressources sélectionnées

Cet exemple configure la correction automatique pour tous les volumes Amazon EBS portant l'ID de Trusted Advisor contrôle DAv U99Dc4C (volumes Amazon EBS sous-utilisés), à l'exception des volumes spécifiés qui ne seront pas corrigés (désignés comme inactifs).

Configurer la correction automatique pour les volumes Amazon EBS portant l'ID de contrôle DAv U99Dc4C, à l'exception des ressources inactives sélectionnées

1. Ouvrez la AWS AppConfig console sur https://console.aws.amazon.com/systems-manager/appconfig.

   Assurez-vous de vous connecter en tant que compte d'administrateur délégué.
2. Sélectionnez Trusted Remediator dans la liste des applications.
3. Choisissez le profil de configuration d'optimisation des coûts.
4. Sélectionnez l'indicateur Amazon EBS Volumes sous-utilisés.
5. Pour le mode d'exécution, sélectionnez Automatisé.
6. Assurez-vous que les manual-for-tagged-onlyattributs automated-for-tagged-onlyet sont vides. Ces attributs sont utilisés pour remplacer le mode d'exécution par défaut pour les ressources dont les balises correspondent.

   Voici un exemple de section Attributs avec des valeurs vides pour automated-for-tagged-onlyet manual-for-tagged-onlyet Automated pour le mode exécution :

7. Choisissez Enregistrer pour mettre à jour la valeur, puis sélectionnez Enregistrer la nouvelle version pour appliquer les modifications. Vous devez sélectionner Enregistrer la nouvelle version pour que Trusted Remediator reconnaisse la modification.

   À ce stade, tous les volumes Amazon EBS sont configurés pour une correction automatique.
8. Ignorez la correction automatique pour certains volumes Amazon EBS :

   a. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

   b. Choisissez Elastic Block Store, Volumes.

   c. Choisissez Tags.

   d. Choisissez Gérer les balises.

e. Ajoutez la balise suivante :

- Clé : DAv TR-U99Dc4C-Mode d'exécution
- Valeur : Inactive

Voici un exemple de section Tags présentant les champs Clé et Valeur :

f. Répétez les étapes 2 à 5 pour tous les volumes Amazon EBS que vous souhaitez exclure de la correction.

Corriger automatiquement les ressources étiquetées

Cet exemple configure la correction automatique pour tous les volumes Amazon EBS dont la balise `Stage=NonProd` porte l'ID de Trusted Advisor vérification DAv U99Dc4C (volumes Amazon EBS sous-utilisés). Toutes les autres ressources dépourvues de cette balise ne sont pas corrigées.

Configurez la correction automatique pour les volumes Amazon EBS avec le tag correspondant à l'ID de contrôle **`Stage=NonProd`** U99Dc4C DAv

1. Ouvrez la AWS AppConfig console sur https://console.aws.amazon.com/systems-manager/appconfig.

   Assurez-vous de vous connecter en tant que compte d'administrateur délégué.
2. Sélectionnez Trusted Remediator dans la liste des applications.
3. Choisissez le profil de configuration d'optimisation des coûts.
4. Sélectionnez l'indicateur Amazon EBS Volumes sous-utilisés.
5. Pour le mode exécution, sélectionnez Conditionnel.
6. Définissez automated-for-tagged-only sur `Stage=NonProd`. Cet attribut remplace la valeur par défaut `execution-mode` pour les ressources dont les balises correspondent. Assurez-vous que les manual-for-tagged-onlyattributs sont vides.

   Voici un exemple de section Attributes automated-for-tagged-onlydéfinie sur Stage= NonProd et Conditional pour le mode exécution :

7. Vous pouvez éventuellement définir les paramètres préconfigurés sur l'une des valeurs suivantes :

- `CreateSnapshot=false`pour ne pas créer de capture instantanée du volume Amazon EBS avant sa suppression
- `MinimumUnattachedDays=10`pour fixer à 10 jours le nombre minimum de jours sans connexion du volume Amazon EBS à supprimer
- `CreateSnapshot=false`, `MinimumUnattachedDays=10` pour les deux options ci-dessus

8. Choisissez Enregistrer pour mettre à jour la valeur, puis sélectionnez Enregistrer la nouvelle version pour appliquer les modifications. Vous devez sélectionner Enregistrer la nouvelle version pour que Trusted Remediator reconnaisse la modification.
9. Assurez-vous que vos volumes Amazon EBS ne comportent pas de balise avec la clé`TR-DAvU99Dc4C-Execution-Mode`. Cette clé de balise remplace le mode d'exécution par défaut pour ce volume EBS.

Travailler avec des corrections dans Trusted Remediator

Suivez les mesures correctives dans Trusted Remediator

Pour suivre OpsItems les mesures correctives, procédez comme suit :

1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Choisissez Gestion des opérations, OpsCenter.
3. (Facultatif) Filtrez la liste par Source=Trusted Remediator pour n'inclure que Trusted Remediator OpsItems dans la liste.

   Voici un exemple d' OpsCenter écran filtré par Source=Trusted Remediator :

> **Note**
>
> Outre la visualisation OpsItems depuis le OpsCenter, vous pouvez consulter les journaux de correction dans le compartiment AMS S3. Pour de plus amples informations, veuillez consulter Journaux de correction dans Trusted Remediator.

Exécutez des corrections manuelles dans Trusted Remediator

Trusted Remediator crée OpsItems des contrôles configurés pour une correction manuelle. Vous devez passer en revue ces vérifications et commencer le processus de correction manuellement.

Pour y remédier manuellement OpsItem, procédez comme suit :

1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Choisissez Gestion des opérations, OpsCenter.
3. (Facultatif) Filtrez la liste par Source=Trusted Remediator pour n'inclure que Trusted Remediator OpsItems dans la liste.
4. Choisissez celui OpsItem que vous souhaitez évaluer.
5. Passez en revue les données opérationnelles du OpsItem. Les données opérationnelles incluent les éléments suivants :
   - trustedAdvisorCheckCatégorie : Catégorie du numéro de Trusted Advisor chèque. Par exemple, Tolérance aux pannes
   - trustedAdvisorCheckID : l'identifiant de Trusted Advisor chèque unique.
   - trustedAdvisorCheckMétadonnées : les métadonnées de la ressource, y compris l'ID de la ressource.
   - trustedAdvisorCheckNom : nom du Trusted Advisor chèque.
   - trustedAdvisorCheckÉtat : état du Trusted Advisor contrôle détecté pour la ressource.
6. Pour y remédier manuellement OpsItem, procédez comme suit :
   a. Dans Runbooks, choisissez l'un des runbooks associés (documents SSM).
   b. Sélectionnez Execute (Exécuter).
   c. Pour AutomationAssumeRole , choisissez `arn:aws:iam::`*`Compte AWS ID`*`:role/ams_ssm_automation_role`. Remplacez l' Compte AWS ID par l'ID du compte sur lequel s'exécute la correction. Pour les autres valeurs de paramètres, consultez les données d'opération.

      Pour corriger manuellement les ressources, le rôle ou l'utilisateur utilisé pour s'authentifier Compte AWS doit disposer des `iam:PassRole` autorisations pour le rôle IAM. `ams-ssm-automation-role` Pour plus d'informations, consultez la section Accorder à un utilisateur

l'autorisation de transmettre un rôle à un architecte cloud Service AWS ou contactez votre architecte cloud.

d. Sélectionnez Execute (Exécuter).

e. Surveillez la progression de l'exécution du document SSM dans la colonne État et résultats les plus récents.

f. Une fois le document terminé, choisissez Définir le statut, Résolu pour résoudre manuellement le OpsItem. Si le document échoue, passez en revue les détails et réexécutez le SSMdocument. Pour obtenir une assistance supplémentaire en matière de dépannage, créez une demande de service.

Pour résoudre un problème OpsItem sans correction, sélectionnez Définir le statut sur Résolu.

7. Répétez les étapes 3 et 4 pour toutes les corrections manuelles restantes. OpsItems

Résoudre les problèmes liés aux mesures correctives dans Trusted Remediator

Pour obtenir de l'aide concernant les corrections manuelles et les défaillances de correction, contactez AMS.

Pour consulter l'état et les résultats de la correction, procédez comme suit :

1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Choisissez Gestion des opérations, OpsCenter.
3. (Facultatif) Filtrez la liste par Source=Trusted Remediator pour n'inclure que Trusted Remediator OpsItems dans la liste.
4. Choisissez celui OpsItem que vous souhaitez évaluer.
5. Dans la section Exécutions automatisées, passez en revue le nom et le statut du document ainsi que les résultats.
6. Passez en revue les défaillances d'automatisation courantes suivantes. Si vos problèmes ne figurent pas dans la liste, contactez votre CSDM pour obtenir de l'aide.

Erreurs de correction courantes

Aucune exécution n'est répertoriée dans Exécutions automatisées

Aucune exécution associée au OpsItem peut indiquer que l'exécution n'a pas pu démarrer en raison de valeurs de paramètres incorrectes.

Étapes de résolution des problèmes

1. Dans les données opérationnelles, vérifiez la valeur de la `trustedAdvisorCheckAutoRemediation` propriété.
2. Vérifiez que les valeurs DocumentNameet Paramètres sont correctes. Pour obtenir les valeurs correctes, consultez Configurer Trusted Advisor la correction des chèques dans Trusted Remediator les informations relatives à la configuration des paramètres SSM. Pour consulter les paramètres de contrôle pris en charge, voir Trusted Advisor contrôles pris en charge par Trusted Remediator
3. Vérifiez que les valeurs du document SSM correspondent aux modèles autorisés. Pour afficher le détail des paramètres dans le contenu du document, sélectionnez le nom du document dans la section Runbooks.
4. Après avoir vérifié et corrigé les paramètres, réexécutez manuellement le document SSM.
5. Pour éviter que cette erreur ne se reproduise, assurez-vous de configurer la correction avec les valeurs de paramètres correctes dans votre configuration. Pour de plus amples informations, consultez Configurer Trusted Advisor la correction des chèques dans Trusted Remediator.

Exécutions ratées dans les exécutions automatisées

Les documents de correction contiennent plusieurs étapes qui interagissent avec l' Services AWS exécution de diverses actions. APIs Pour identifier la cause spécifique de l'échec, procédez comme suit :

Étapes de résolution des problèmes

1. Pour afficher les différentes étapes d'exécution, choisissez l'ID d'exécution, lien dans la section Exécutions automatisées. Voici un exemple de console Systems Manager illustrant les étapes d'exécution d'une automatisation sélectionnée :

2. Choisissez l'étape dont le statut a échoué. Voici des exemples de messages d'erreur :

   - `NoSuchBucket - An error occurred (NoSuchBucket) when calling the GetPublicAccessBlock operation: The specified bucket does not exist`

Cette erreur indique que le nom de compartiment spécifié dans les paramètres préconfigurés de la configuration de correction est incorrect.

Pour résoudre cette erreur, exécutez manuellement l'automatisation en utilisant le nom de compartiment correct. Pour éviter que ce problème ne se reproduise, mettez à jour la configuration de correction avec le nom de compartiment correct.

- `DB instance my-db-instance-1 is not in available status for modification.`

  Cette erreur indique que l'automatisation n'a pas pu apporter les modifications attendues car l'état de l'instance de base de données n'était pas valide.

  Pour résoudre cette erreur, exécutez manuellement l'automatisation.

Journaux de correction dans Trusted Remediator

Trusted Remediator crée des journaux au format JSON et les télécharge sur Amazon Simple Storage Service. Les fichiers journaux sont chargés dans un compartiment S3 créé par AMS et nommé. `ams-trusted-remediator-{your-account-id}-logs` AMS crée le compartiment S3 dans le compte d'administrateur délégué. Vous pouvez importer les fichiers journaux QuickSight pour générer des rapports de correction personnalisés.

Pour de plus amples informations, veuillez consulter Intégration de Trusted Remediator avec QuickSight.

Journal des éléments de correction

Trusted Remediator crée le `Remediation item log` lorsqu'une correction OpsItem est créée. Ce journal contient les corrections manuelles OpsItem et les corrections automatisées. OpsItem Vous pouvez utiliser le `Remediation item log` pour suivre la vue d'ensemble de toutes les mesures correctives.

Emplacement du journal des éléments de correction pour les recommandations de Compute Optimizer

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs/compute_optimizer_remediation_items/`*`remediation creation time in yyyy-mm-`*

dd format/*10 digits epoch time or unix timestamp*-*Trusted Advisor check ID*-*Resource ID*.json

Emplacement du journal des éléments de correction pour les vérifications Trusted Advisor

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs/remediation_items/*remediation creation time in yyyy-mm-dd format*/*10 digits epoch time or unix timestamp*-*Trusted Advisor check ID*- *Resource ID*.json

URL du fichier d'exemple du journal des éléments de correction

s3:///ams-trusted-remediator-*111122223333*-logs/remediation_items/*2023-02-06*/*1675660464-DAvU99Dc4C-vol-00bd8965660b4c16d.json*

Format du journal des éléments de remédiation de Compute Optimizer

```
{
  "AccountID": "Account_ID",
  "ComputeOptimizerCheckID": "Compute Optimizer check ID",
  "ComputeOptimizerCheckName": "Compute Optimizer check name",
  "ResourceID": "Resource ID",
  "RemediationTime": Remediation creation time,
  "ExecutionMode": "Automated or Manual",
  "OpsItemID": "OpsItem ID"
}
```

Trusted Advisor Format du journal des éléments de correction

```
{
   "TrustedAdvisorCheckID": Trusted Advisor check ID,
   "TrustedAdvisorCheckName": Trusted Advisor check name,
   "TrustedAdvisorCheckResultTime": 10 digits epoch time or unix timestamp,
   "ResourceID": Resource ID,
   "RemediationTime": Remediation creation time,
   "ExecutionMode": Automated or Manual,
   "OpsItemID": OpsItem ID
}
```

Exemple de contenu du journal des éléments de Compute Optimizer Remediation

```
{
```

```
  "AccountID": "123456789012",
  "ComputeOptimizerCheckID": "compute-optimizer-ebs",
  "ComputeOptimizerCheckName": "EBS volumes",
  "ResourceID": "vol-1235589366f77aca7",
  "RemediationTime": 1755044783,
  "ExecutionMode": "Manual",
  "OpsItemID": "oi-b8888b38fe78"
}
```

Trusted Advisor Exemple de contenu au format du journal des éléments de correction

```
{
    "TrustedAdvisorCheckID": "DAvU99Dc4C",
    "TrustedAdvisorCheckName": "Underutilized Amazon EBS Volumes",
    "TrustedAdvisorCheckResultTime": 1675614749,
    "ResourceID": "vol-00bd8965660b4c16d",
    "RemediationTime": 1675660464,
    "OpsItemID": "oi-cca5df7af718"
}
```

Journal d'exécution automatique des mesures correctives, Compute Optimizer et Trusted Advisor

Trusted Remediator crée le `Automated remediation execution log` lorsqu'un document SSM est exécuté automatiquement. Ce journal contient les détails de l'exécution du SSM pour la correction automatique uniquement. OpsItem Vous pouvez utiliser ce fichier journal pour suivre les corrections automatisées.

Compute Optimizer Localisation automatique des journaux de correction

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs//remediation_executions/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Compute Optimizer recommendation ID`*`.json`

Trusted Advisor Emplacement automatique des journaux de correction

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs//remediation_executions/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Trusted Advisor check ID`*`-`*`Resource ID`*`.json`

Exemple de localisation du journal de correction automatisé Compute Optimizer

`s3://ams-trusted-remediator-111122223333-logs/remediation_executions/2025-06-26/1750908858-123456789012-compute-optimizer-ec2-i-1235173471d2cd789.json`

Trusted Advisor Exemple de localisation automatique du journal de correction

`s3://ams-trusted-remediator-111122223333-logs/remediation_executions/2023-02-06/1675660573-DAvU99Dc4C-vol-00bd8965660b4c16d.json`

Exemple de contenu au format du journal de correction automatisé

```
{
    "OpsItemID": "oi-767c77e05301",
    "SSMExecutionID": "93d091b2-778a-4cbc-b672-006954d76b86",
    "SSMExecutionStatus": "Success"}
```

Journal des comptes des membres

Trusted Remediator crée le `Member accounts log` lorsque votre compte est intégré ou déconnecté. Vous pouvez utiliser le `Member accounts log` pour trouver l'identifiant du compte, le numéro d'enregistrement et Régions AWS l'heure d'exécution de chaque compte membre.

Emplacement du journal des comptes membres

`s3://ams-trusted-remediator-delegated-administrator-account-id-logs/configuration_logs/member_accounts.json`

URL du fichier d'exemple du journal des comptes membres

`s3://ams-trusted-remediator-111122223333-logs/configuration_logs/member_accounts.json`

Format du journal des comptes membres

```
{
    "delegated_administrator_account_id": Delegated Administrator account id,
    "appconfig_configuration_region": Trusted Remediator AppConfig Region,
    "member_accounts": [
```

```
        {
            "account_id": Member account id
            "account_partition": Member account partition (for example, aws),
            "regions": [
                {
                    "execution_time": Remediation execution time in cron schedule
 expression,
                    "execution_timezone": Timezone for the remediation execution time,
                    "region_name": Région AWS name
                }
                ...
            ]
        }
        ...
    ],
    "updated_at": Log update time,
}
```

Exemple de contenu du format du journal des comptes membres

```
{
    "delegated_administrator_account_id": "111122223333",
    "appconfig_configuration_region": "ap-southeast-2",
    "member_accounts": [
        {
            "account_id": "222233334444",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 9 * * 6",
                    "execution_timezone": "Australia/Sydney",
                    "region_name": "ap-southeast-2"
                },
                {
                    "execution_time": "0 5 * * 7",
                    "execution_timezone": "UTC",
                    "region_name": "us-east-1"
                }
            ]
        },
        {
            "account_id": "333344445555",
            "account_partition": "aws",
```

```
            "regions": [
                {
                    "execution_time": "0 1 * * 5",
                    "execution_timezone": "Asia/Seoul",
                    "region_name": "ap-northeast-2"
                }
            ]
        }
    ],
    "updated_at": "1730869607"
}
```

Intégration de Trusted Remediator avec QuickSight

Vous pouvez intégrer les journaux Trusted Remediator stockés dans Amazon S3 QuickSight pour créer un rapport de correction personnalisé. QuickSight l'intégration est facultative. Cette fonctionnalité vous permet d'utiliser les journaux pour créer des tableaux de bord de rapports personnalisés. Pour obtenir des rapports sur demande pour Trusted Remediator, contactez votre CSDM. Pour plus d'informations sur les rapports Trusted Remediator disponibles, consultezRapports Trusted Remediator.

Pour plus d'informations sur la visualisation des données dans QuickSight, voir Visualisation des données dans. QuickSight

Ajouter un ensemble de données QuickSight pour le journal des éléments de correction

Pour ajouter un ensemble de données au QuickSight journal des éléments de correction, procédez comme suit :

1. Connectez-vous à la QuickSight console. Vous pouvez créer le QuickSight rapport dans n'importe quel Région AWS QuickSight support. Toutefois, pour améliorer les performances et réduire les coûts, il est recommandé de créer le rapport dans la région où se trouve le bucket de journalisation Trusted Remediator.
2. Choisissez Datasets.
3. Choisissez S3.
4. Dans la nouvelle source de données S3, entrez les valeurs suivantes :

- Nom de la source de données : `trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-items`
- Téléchargez un fichier manifeste : créez un fichier JSON avec le contenu suivant et utilisez-le. Lors de la création du fichier, remplacez-le `logging_bucket_name` dans la URIPrefixes clé.

```
{
    "fileLocations": [
        {
            "URIPrefixes": [
                "s3://{logging_bucket_name}/remediation_items/"
            ]
        }
    ],
    "globalUploadSettings": {
        "format": "JSON",
        "delimiter": ",",
        "textqualifier": "'",
        "containsHeader": "true"
    }
}
```

- Choisissez Se connecter.
- Dans la fenêtre Terminer la création du jeu de données, choisissez Visualize.
- QuickSight ouvre la nouvelle page de la feuille d'analyse. Vous êtes maintenant prêt à créer une nouvelle analyse à l'aide du journal des éléments de correction.

Voici un exemple d'analyse :

Ajouter un ensemble de données QuickSight pour le journal d'exécution des mesures correctives automatisées

1. Connectez-vous à la QuickSight console. Vous pouvez créer le QuickSight rapport dans n'importe quel Région AWS QuickSight support. Toutefois, pour améliorer les performances et réduire les coûts, il est recommandé de créer le rapport dans la région où se trouve le bucket de journalisation Trusted Remediator.
2. Choisissez Datasets.

3. Choisissez S3.
4. Dans la nouvelle source de données S3, entrez les valeurs suivantes :

   - Nom de la source de données : `trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-executions`
   - Téléchargez un fichier manifeste : créez un fichier JSON avec le contenu suivant, puis utilisez-le. Lors de la création du fichier, remplacez-le `logging_bucket_name` dans la URIPrefixes clé.

     ```
     {
         "fileLocations": [
             {
                 "URIPrefixes": [
                     "s3://{logging_bucket_name}/remediation_executions/"
                 ]
             }
         ],
         "globalUploadSettings": {
             "format": "JSON",
             "delimiter": ",",
             "textqualifier": "'",
             "containsHeader": "true"
         }
     }
     ```

   - Choisissez Se connecter.
   - Dans la fenêtre Terminer la création du jeu de données, choisissez Visualize.
   - QuickSight ouvre la nouvelle page de la feuille d'analyse. Vous êtes maintenant prêt à créer une nouvelle analyse à l'aide du journal des éléments de correction.

Voici un exemple d'analyse :

Meilleures pratiques en matière de Trusted Remediator

Voici les meilleures pratiques qui vous aideront à utiliser Trusted Remediator :

- Si vous n'êtes pas sûr des résultats de la correction, commencez par le mode d'exécution manuelle. Parfois, l'application de l'exécution automatique des mesures correctives dès le départ peut entraîner des résultats inattendus.
- Réalisez un examen hebdomadaire des mesures correctives et obtenez des informations sur OpsItems les résultats de Trusted Remediator.
- Les comptes membres héritent des configurations du compte d'administrateur délégué. Il est donc important de structurer les comptes de manière à vous aider à gérer plusieurs comptes avec les mêmes configurations. Vous pouvez exempter les ressources de la configuration par défaut à l'aide de balises.

Correcteur fiable FAQs

Les questions fréquemment posées à propos de Trusted Remediator sont les suivantes :

Qu'est-ce que Trusted Remediator et quels en sont les avantages pour moi ?

Lorsqu'une non-conformité est identifiée Trusted Advisor ou qu'une recommandation est émise par Compute Optimizer, Trusted Remediator répond en fonction de vos préférences, soit en appliquant des mesures correctives, soit en demandant l'approbation par le biais de corrections manuelles, soit en signalant les mesures correctives lors de votre prochaine revue commerciale mensuelle (MBR). La correction a lieu à l'heure ou au calendrier de correction que vous préférez. Trusted Remediator vous permet de gérer les contrôles en libre-service et d'agir en fonction Trusted Advisor des contrôles, tout en vous permettant de configurer et de corriger les contrôles de manière individuelle ou groupée. Avec une bibliothèque de documents de correction testés, AMS augmente constamment vos comptes en appliquant des contrôles de sécurité et en suivant les AWS meilleures pratiques. Vous n'êtes averti que si vous le spécifiez dans votre configuration. Les utilisateurs d'AMS peuvent souscrire à Trusted Remediator sans frais supplémentaires.

Quels sont les liens entre Trusted Remediator et les autres ? Services AWS

Vous avez accès aux Trusted Advisor vérifications et aux recommandations de Compute Optimizer dans le cadre de votre plan Enterprise Support existant. Trusted Remediator s'intègre à Compute Optimizer Trusted Advisor et s'intègre à Compute Optimizer pour tirer parti des capacités d'automatisation AMS existantes. En particulier, AMS utilise des documents AWS Systems Manager d'automatisation (runbooks) pour les corrections automatisées. AWS AppConfig est utilisé pour configurer les flux de travail de correction. Vous pouvez consulter toutes les corrections actuelles et passées via le Systems Manager OpsCenter. Les journaux de correction sont stockés dans un

compartiment Amazon S3. Vous pouvez utiliser les journaux pour importer et créer des tableaux de bord de rapports personnalisés. QuickSight

Qui configure les mesures correctives ?

Vous êtes propriétaire des configurations de votre compte. La gestion de vos configurations est de votre responsabilité. Vous pouvez contacter votre CA ou votre CDSM pour obtenir de l'aide pour gérer vos configurations. Vous pouvez également contacter AMS par le biais d'une demande de service pour obtenir une assistance à la configuration, des corrections manuelles et le dépannage des défaillances liées aux mesures correctives.

Comment installer des documents d'automatisation SSM ?

Les documents d'automatisation SSM sont automatiquement partagés avec les comptes AMS intégrés.

Les ressources détenues par AMS seront-elles également corrigées ?

Les ressources détenues par AMS ne sont pas signalées par Trusted Remediator. Trusted Remediator se concentre uniquement sur vos ressources.

Qu' Régions AWS est-ce que Trusted Remediator est disponible et qui peut l'utiliser ?

Trusted Remediator est disponible pour les clients d'AMS Accelerate. Pour consulter la liste actuelle des régions prises en charge, voir Services AWS par région.

Trusted Remediator provoquera-t-il une dérive des ressources ?

Étant donné que les documents d'automatisation SSM mettent directement à jour les ressources via l' AWS API, une dérive des ressources peut se produire. Vous pouvez utiliser des balises pour séparer les ressources créées par le biais de vos packages existants CI/CD . Vous pouvez configurer Trusted Remediator pour ignorer les ressources balisées tout en corrigeant vos autres ressources.

Comment suspendre ou arrêter Trusted Remediator ?

Vous pouvez désactiver Trusted Remediator via l' AWS AppConfig application. Pour suspendre ou arrêter Trusted Remediator, procédez comme suit :

1. Ouvrez la AWS AppConfig console sur https://console.aws.amazon.com/systems-manager/appconfig.
2. Sélectionnez Trusted Remediator.

3. Choisissez Paramètres dans le profil de configuration.
4. Sélectionnez l'indicateur Suspend Trusted Remediator.
5. Définissez la valeur de l'`suspended`attribut sur. `true`

> **Note**
>
> Soyez prudent lorsque vous utilisez cette procédure, car cela arrête Trusted Remediator pour tous les comptes liés au compte d'administrateur délégué.

Comment puis-je corriger les vérifications qui ne sont pas prises en charge par Trusted Remediator ?

Vous pouvez continuer à contacter AMS via Operations On Demand (OOD) pour les chèques non pris en charge. AMS vous aide à corriger ces contrôles. Pour plus d'informations, consultez la section Opérations à la demande.

En quoi Trusted Remediator est-il différent de la AWS Config remédiation ?

AWS Config La correction est une autre solution qui vous aide à optimiser les ressources du cloud et à maintenir la conformité aux meilleures pratiques. Voici certaines des différences opérationnelles entre les deux solutions :

- Trusted Remediator utilise Trusted Advisor Compute Optimizer comme mécanismes de détection. AWS Config La correction utilise des AWS Config règles comme mécanisme de détection.
- Pour Trusted Remediator, la correction s'effectue selon votre calendrier de remédiation prédéfini. En AWS Config, la remédiation se fait en temps réel.
- Les paramètres de chaque correction dans Trusted Remediator sont facilement personnalisables en fonction de votre cas d'utilisation et la correction peut être automatisée ou rendue manuelle en ajoutant des balises sur les ressources.
- Trusted Remediator fournit des fonctionnalités de reporting.
- Trusted Remediator vous envoie une notification par e-mail contenant la liste des mesures correctives et leur état.

Certaines Trusted Advisor vérifications et recommandations de Compute Optimizer peuvent comporter la même règle. AWS Config Il est recommandé de n'activer qu'une seule correction s'il existe une AWS Config règle et une Trusted Advisor vérification correspondantes. Pour plus

d'informations sur AWS Config les règles applicables à chaque Trusted Advisor contrôle, voirTrusted Advisor contrôles pris en charge par Trusted Remediator.

Quelles ressources Trusted Remediator déploie-t-il sur vos comptes ?

Trusted Remediator déploie les ressources suivantes sur le compte d'administrateur délégué de Trusted Remediator :

- Un compartiment Amazon S3 nomméams-trusted-remediator-{your-account-id}-logs. Trusted Remediator crée le fichier Remediation item log au format JSON lorsqu'une correction OpsItem est créée et télécharge les fichiers journaux dans ce compartiment.
- Une AWS AppConfig application qui contient les configurations de correction pour les Trusted Advisor vérifications prises en charge et les recommandations de Compute Optimizer.

Trusted Remediator ne déploie pas de ressources sur le compte membre Trusted Remediator.

Surveillance et gestion des incidents pour Amazon EKS dans AMS Accelerate

La surveillance et la gestion des incidents pour Amazon EKS surveillent vos ressources Amazon EKS pour détecter les défaillances, la dégradation des performances et les problèmes de sécurité. AMS Accelerate configure et déploie les règles du gestionnaire d'alertes Amazon Managed Service for Prometheus, surveille les alertes, puis gère les incidents lorsque ces alertes sont déclenchées. La surveillance et la gestion des incidents pour Amazon EKS s'appuient sur AMS Alarm Manager et s'appuient sur AWS des services natifs, tels qu'Amazon Managed Service for Prometheus, Amazon Managed Grafana, Amazon et. GuardDuty AWS LambdaAWS Config

> **Note**
>
> La surveillance et la gestion des incidents pour Amazon EKS ne sont pas AWS GovCloud (US) compatibles avec les nœuds Windows ou les conteneurs Windows.

Qu'est-ce que la surveillance et la gestion des incidents pour Amazon EKS dans AMS Accelerate ?

La surveillance et la gestion des incidents pour Amazon EKS fournissent les éléments suivants :

- Configuration par défaut qui crée, gère et déploie des moniteurs et des politiques sur votre compte géré pour les clusters Amazon EKS que vous sélectionnez.
- Une base de surveillance pour permettre à vos charges de travail Amazon EKS d'augmenter la disponibilité, même si vous ne configurez aucune autre surveillance pour vos clusters Amazon EKS. Pour de plus amples informations, veuillez consulter Alertes de base en matière de surveillance et de gestion des incidents pour Amazon EKS dans AMS Accelerate.
- Notifications générées par la surveillance de base configurée pour votre cluster Amazon EKS. Ces notifications sont appelées alertes. Des alertes sont générées en cas de défaillances imminentes, continues, récurrentes ou potentielles, de dégradation des performances ou de problèmes de sécurité. Les alertes incluent par exemple une alerte Prometheus, un événement ou une découverte provenant d' AWS un service tel qu'Amazon. GuardDuty

- Enquête d'alerte avec des conseils sur les mesures correctives appropriées que vous pouvez prendre. Pour plus d'informations, consultez la section Rapports d'incidents et demandes de service dans AMS Accelerate.
- Correction des alertes et des incidents par les opérations AMS, lorsque cela est possible et avec votre approbation, afin de prévenir ou de réduire l'impact sur vos applications. Pour plus d'informations, consultez la section Rapports d'incidents et demandes de service dans AMS Accelerate.
- Tableaux de bord Amazon Managed Grafana prédéfinis facultatifs qui fournissent une visibilité sur l'utilisation des ressources, les performances, l'état de CoreDNS, les alertes actives et les alertes précédemment résolues. Si vous configurez Amazon Managed Grafana à l'aide du modèle fourni par AMS, vous pouvez ouvrir la console Amazon Managed Grafana pour consulter les métriques et les alertes de votre cluster Amazon EKS.

Comment fonctionnent la surveillance et la gestion des incidents pour Amazon EKS dans AMS Accelerate

Génération : dans le cadre de la surveillance de l'intégration et de la gestion des incidents pour EKS, AMS configure la surveillance de base pour les clusters Amazon EKS que vous avez sélectionnés dans votre compte géré. AMS utilise une combinaison des règles du gestionnaire d'alertes Amazon Managed Service for Prometheus et des règles relatives aux événements CloudWatch Amazon pour configurer la surveillance de base. Un serveur Prometheus configuré par AMS dans votre cluster récupère et écrit à distance vos métriques Prometheus sur un point de terminaison Amazon Managed Service for Prometheus situé dans la même région. La configuration de surveillance de base génère une alerte lorsqu'une règle du gestionnaire d'alertes Prometheus est déclenchée ou qu' CloudWatch un événement est généré.

Agrégation : AMS envoie toutes les alertes générées par vos ressources au système de surveillance AMS en les dirigeant vers une rubrique Amazon Simple Notification Service gérée par AMS.

Traitement et analyse d'impact : AMS analyse les alertes puis les traite en fonction de leur impact potentiel. AMS classe les alertes comme suit :

- Alertes ayant un impact connu sur le client : pour ces alertes, AMS crée un nouveau rapport d'incident en utilisant le processus de gestion des incidents.
- Alertes dont l'impact sur le client est incertain : pour ces alertes, AMS envoie un rapport d'incident. Dans de nombreux cas, ces alertes vous demandent de vérifier l'impact avant qu'AMS ne puisse

agir. Pour de telles alertes, AMS envoie une notification d'alerte avec les détails et vérifie si l'alerte nécessite une action d'atténuation. AMS fournit des options pour atténuer les actions dans la notification. Si votre réponse confirme que l'alerte est un incident, AMS déclenche alors la création d'un nouveau rapport d'incident et lance le processus de gestion des incidents. Toute notification de service qui reçoit une réponse indiquant « aucune incidence sur le client » ou aucune réponse pendant trois jours est considérée comme résolue. De plus, l'alerte correspondante est marquée comme résolue.

- Alertes sans impact sur le client : si, après évaluation, AMS détermine que l'alerte n'a aucun impact sur le client, l'alerte est fermée.

Matrice de responsabilité AMS (RACI)

La matrice AMS responsable, responsable, consultée et informée, ou matrice RACI, attribue la responsabilité principale au client ou à AMS pour diverses activités. Le tableau suivant fournit un aperçu des responsabilités du client et d'AMS en ce qui concerne les activités d'une application qui utilise la surveillance et la gestion des incidents pour Amazon EKS.

- R représente la partie responsable qui fait le travail pour accomplir la tâche.
- A représente la partie responsable.
- C signifie consulté, c'est-à-dire la partie dont l'opinion est sollicitée, généralement en tant qu'expert en la matière, et avec laquelle il existe une communication bilatérale.
- I signifie informé, c'est-à-dire la partie qui est informée des progrès, souvent uniquement une fois la tâche ou le résultat livrable terminé.

Activité	Client	AMS
Exigences relatives à Discovery for AMS	I	R
Activer les autorisations AMS (RBAC) pour l'accès au cluster	R	C
Installez l'agent Amazon EC2 Systems Manager sur les	R	C

Activité	Client	AMS
nœuds de travail s'il n'est pas déjà présent		
Déployez des composant s AMS sur le cluster, tels que Prometheus, Prometheu s Node kube-state-metrics Exporter, et dans un espace de noms AMS, selon les besoins.	C	R
Fournir Amazon Managed Service pour Prometheus dans le plan de contrôle AMS	I	R
Configurer le gestionnaire d'alertes Prometheus dans le plan de contrôle AMS	I	R
Fournissez le modèle Amazon Managed Grafana et aidez à la configuration	C	R
Activer la surveillance du journal d'audit GuardDuty EKS	C	R
Activer la journalisation du plan de contrôle Amazon EKS	I	R
Surveillez l'état et les performances du plan de contrôle Amazon EKS	I	R

Activité	Client	AMS
Surveillez l'état et les performances de votre cluster Amazon EKS (cluster, nœud, charge de travail, module, serveur d'API et CoreDNS)	I	R
Triez les alertes et répondez aux incidents pour Amazon EKS	I	R
Exécuter des commandes de diagnostic lors d'incidents	I	R
Analyser les journaux lors d'incidents (journaux du plan de contrôle et du pod)	I	R
Réponse aux incidents en cas de problèmes AWS de réseau	I	R
Répondre aux résultats de surveillance du journal d'audit GuardDuty EKS	I	R
Fournir des conseils aux clients sur les mesures à prendre pour remédier aux incidents lorsque cela est possible	I	R

Alertes de base en matière de surveillance et de gestion des incidents pour Amazon EKS dans AMS Accelerate

Après avoir vérifié les alertes, AMS active les alertes suivantes pour Amazon EKS, puis se charge de la surveillance et de la gestion des incidents pour les clusters Amazon EKS que vous avez

sélectionnés. Le temps de réponse des accords de niveau de service (SLAs) et les objectifs de niveau de service (SLOs) dépendent du niveau de service (Plus, Premium) que vous avez sélectionné pour votre compte. Pour plus d'informations, consultez la section Rapports d'incidents et demandes de service dans AMS Accelerate.

Alertes et actions

Le tableau suivant répertorie les alertes Amazon EKS et les actions respectives entreprises par AMS :

Alerte	Seuils	Action
Container OOM tué	Le nombre total de redémarrages de conteneurs au cours des 10 dernières minutes est d'au moins 1 et un conteneur Kubernetes d'un pod a été fermé avec le motif « OOMKilled » au cours des 10 dernières minutes.	AMS cherche à déterminer si le kill OOM est dû à l'atteinte de la limite de conteneur ou à un dépassement de la limite de mémoire, puis vous conseille sur les mesures correctives à prendre.
Pod Job a échoué	Une tâche Kubernetes échoue. L'échec est indiqué par la présence d'au moins un statut d'échec de la tâche.	AMS étudie les raisons de l'échec de la tâche Kubernetes ou de la tâche cron correspondante, puis vous conseille sur les mesures correctives à prendre.
StatefulSet Vers le bas	Le nombre de répliques prêtes à servir le trafic ne correspond pas au nombre actuel de répliques existantes StatefulSet pendant au moins 1 minute.	AMS détermine pourquoi les pods ne sont pas prêts en consultant les messages d'erreur dans les événements des pods et les extraits du journal des erreurs dans les logs des pods, puis vous conseille sur les mesures correctives à prendre.

Alerte	Seuils	Action
Capacité de mise à l'échelle HPA	L'Horizontal Pod Autoscaler (HPA) ne peut pas être redimensionné car la condition d'état « AbleToScale » est fausse pendant au moins 2 minutes.	AMS détermine quel Kubernetes Horizontal Pod Autoscaler (HPA) n'est pas en mesure de dimensionner les pods pour la ressource de charge de travail suivante, telle qu'un déploiement ou. StatefulSet
Disponibilité des métriques HPA	L'Horizontal Pod Autoscaler (HPA) ne peut pas collecter de mesures car la condition d'état « ScalingActive » est fausse pendant au moins 2 minutes.	AMS détermine pourquoi HPA ne peut pas collecter de métriques, telles que les métriques liées aux problèmes de configuration du serveur ou aux problèmes d'autorisation RBAC.
Le pod n'est pas prêt	Un pod Kubernetes reste dans un état non actif (tel que En attente, Inconnu ou Échoué) pendant plus de 15 minutes.	AMS enquête sur le ou les pods concernés pour plus de détails, examine les journaux des pods pour détecter les erreurs et les événements associés, puis vous conseille sur les mesures correctives à prendre.

Alerte	Seuils	Action
Pod Crash en boucle	Un conteneur à capsules redémarre au moins une fois toutes les 15 minutes pendant une heure.	AMS étudie les raisons pour lesquelles le pod ne démarre pas, telles que des ressources insuffisantes, un fichier verrouillé par un autre conteneur, une base de données verrouillée par un autre conteneur, l'échec des dépendances de service, des problèmes de DNS pour les services externes et des erreurs de configuration.
Daemonset mal planifié	Au moins un pod Kubernete s Daemonset a été mal planifié sur une période de 10 minutes.	AMS détermine pourquoi un Daemonset est planifié sur un nœud où il n'est pas censé s'exécuter. Cela peut se produire lorsque le mauvais pod a nodeSelector/taints/ affinities été appliqué aux pods Daemonset ou lorsque le nœud (pool de nœuds) a été contaminé et que l'expulsion des pods existants n'a pas été planifiée.

Alerte	Seuils	Action
Erreurs d'API Kubernetes	Le taux d'erreur du serveur d'API Kubernetes dépasse 3 % sur une période de 2 minutes.	AMS analyse les journaux du plan de contrôle pour déterminer le volume et le type d'erreurs à l'origine de cette alerte, et identifie tout problème de contention des ressources pour les nœuds principaux ou les groupes de mise à l'échelle automatique etcd. Si le serveur d'API ne se rétablit pas, AMS fait appel à l'équipe de service Amazon EKS.
Latence de l'API Kubernetes	Le 99e percentile de latence des demandes adressées au serveur d'API Kubernetes dépasse 1 seconde sur une période de 2 minutes.	AMS analyse les journaux du plan de contrôle pour déterminer le volume et les types d'erreurs à l'origine de la latence et identifie tout problème de contention des ressources pour les nœuds principaux ou les groupes d'auto-scaling etcd. Si le serveur d'API ne se rétablit pas, AMS fait appel à l'équipe de service Amazon EKS.
Expiration du certificat client Kubernetes	Le certificat client utilisé pour s'authentifier auprès du serveur d'API Kubernetes expirera dans moins de 24 heures.	AMS envoie cette notification pour vous informer que votre certificat de cluster expirera dans 24 heures.

Alerte	Seuils	Action
Le nœud n'est pas prêt	Le statut « Prêt » du nœud est faux pendant au moins 10 minutes.	AMS étudie les conditions et les événements du nœud, tels que les problèmes de réseau, qui empêchent l'accès de Kubelet au serveur API.
Processeur Node High	La charge du processeur dépasse 80 % sur une période de 5 minutes.	AMS détermine si un ou plusieurs pods consommen t une quantité anormalem ent élevée de CPU. AMS vérifie ensuite avec vous que vos demandes, vos limites et l'activité de vos pods sont conformes aux attentes.
Node OOM Kill détecté	Au moins un kill OOM de l'hôte est signalé par le nœud dans une fenêtre de 4 minutes.	AMS détermine si le kill OOM est dû à l'atteinte de la limite de conteneur ou au dépassement du nombre de nœuds. Si l'activité de l'applica tion est normale, AMS vous conseille sur les demandes et les limites relatives aux survalidations et à la révision des limites de pods.

Alerte	Seuils	Action
Limite de connexion aux nœuds	Le rapport entre le nombre actuel d'entrées de suivi des connexions et la limite maximale dépasse 80 % sur une période de 5 minutes.	AMS vous conseille sur la valeur de conntrack recommandée par cœur. Les nœuds Kubernetes définissent la valeur maximale de conntrack proportio nnellement à la capacité de mémoire totale du nœud. Les applications à charge élevée, en particulier sur les petits nœuds, peuvent facilement dépasser la valeur maximale de conntrack, ce qui entraîne des réinitialisations de connexion et des délais d'attente.
L'horloge du nœud n'est pas synchronisée	L'état de synchronisation minimal sur une période de 2 minutes est 0, et l'erreur maximale en secondes est de 16 ou plus.	AMS détermine si le protocole NTP (Network Time Protocol) est installé et fonctionne correctement.
Processeur Pod High	L'utilisation du processeur d'un conteneur dépasse 80 % sur une fréquence de 3 minutes pendant une période minimale de 2 minutes.	AMS analyse les journaux du pod pour déterminer les tâches du pod qui consommen t une grande quantité de processeur.
Pod High Memory	L'utilisation de la mémoire d'un conteneur dépasse 80 % de la limite de mémoire spécifiée sur une période de 2 minutes.	AMS analyse les journaux du pod pour déterminer les tâches du pod qui consommen t une grande quantité de mémoire.

Alerte	Seuils	Action
CoreDNS en panne	CoreDNS a disparu de la découverte de la cible de Prometheus pendant plus de 15 minutes.	Il s'agit d'une alerte critique qui indique que la résolutio n des noms de domaine pour les services de cluster internes ou externes s'est arrêtée. AMS vérifie l'état des pods CoreDNS, vérifie la configuration CoreDNS, vérifie les points de terminais on DNS qui pointent vers des pods CoreDNS, vérifie les limites CoreDNS et, avec votre approbation, active la journalis ation du débogage CoreDNS.
Erreurs CoreDNS	CoreDNS renvoie des erreurs SERVFAIL pour plus de 3 % des requêtes DNS sur une période de 10 minutes.	Cette alerte peut signaler un problème lié à une applicati on ou une mauvaise configura tion. AMS vérifie l'état des pods CoreDNS, vérifie la configuration CoreDNS, vérifie les points de terminaison DNS qui pointent vers des pods CoreDNS, vérifie les limites CoreDNS et, avec votre approbation, active la journalis ation du débogage CoreDNS.

Alerte	Seuils	Action
Latence CoreDNS	Le 99e percentile des durées de requête DNS dépasse 4 secondes pendant 10 minutes.	Cette alerte indique que CoreDNS est peut-être surchargé. AMS vérifie l'état des pods CoreDNS, vérifie la configuration CoreDNS, vérifie les points de terminais on DNS qui pointent vers les pods CoreDNS, vérifie les limites CoreDNS et, avec votre approbation, active la journalis ation du débogage CoreDNS.
Latence de transfert CoreDNS	Le 99e percentile du temps de réponse des demandes de transfert CoreDNS à kube-DNS dépasse 4 secondes sur une période de 10 minutes.	Lorsque CoreDNS n'est pas le serveur faisant autorité ou ne possède pas d'entrée de cache pour un nom de domaine, CoreDNS transmet la demande DNS à un serveur DNS en amont. Cette alerte indique que CoreDNS est peut-être surchargé ou qu'il peut y avoir un problème avec un serveur DNS en amont. AMS vérifie l'état des pods CoreDNS, vérifie la configura tion CoreDNS, vérifie les points de terminaison DNS qui pointent vers des pods CoreDNS, vérifie les limites CoreDNS et, avec votre approbation, active la journalis ation du débogage CoreDNS.

Alerte	Seuils	Action
Erreur de transfert CoreDNS	Plus de 3 % des requêtes DNS échouent sur une période de 5 minutes.	Lorsque CoreDNS n'est pas le serveur faisant autorité ou ne possède pas d'entrée de cache pour un nom de domaine, CoreDNS transmet la demande DNS à un serveur DNS en amont. Cette alerte signale une éventuell e erreur de configuration ou un problème avec un serveur DNS en amont. AMS vérifie l'état des pods CoreDNS, vérifie la configura tion CoreDNS, vérifie les points de terminaison DNS qui pointent vers des pods CoreDNS, vérifie les limites CoreDNS et, avec votre approbation, active la journalis ation du débogage CoreDNS.

Exigences relatives à la surveillance et à la gestion des incidents pour Amazon EKS dans AMS Accelerate

Voici les ressources and/or nécessaires prises en charge pour la surveillance et la gestion des incidents pour Amazon EKS for AMS Accelerate

- Versions de Kubernetes prises en charge : consultez les versions d'Amazon EKS Kubernetes dans le guide de l'utilisateur d'Amazon EKS.
- Types de nœuds : les nœuds gérés par Amazon EKS sont pris en charge. Les nœuds et conteneurs Windows ne sont pas pris en charge.
- Accès au cluster Kubernetes : AMS nécessite le rôle de cluster RBAC system:masters et l'utilisateur du cluster.

- Agent SSM sur les EC2 nœuds Amazon : L'agent SSM est préinstallé sur Bottle Rocket et Amazon EKS AMIs . Assurez-vous que l'agent SSM est installé sur vos EC2 nœuds personnalisés AMIs et Amazon.
- Quotas de service Pour plus d'informations, consultez les quotas de service pour Amazon Managed Service for Prometheus et Amazon Managed Grafana.
- AWS Régions prises en charge :

Nom de la région	Region (Région)	Région de stockage des métriques
USA Est (Ohio)	us-east-2	us-east-2
USA Est (Virginie du Nord)	us-east-1	us-east-1
USA Ouest (Oregon)	us-west-2	us-west-2
Asie-Pacifique (Tokyo)	ap-northeast-1	ap-northeast-1
Asie-Pacifique (Séoul)	ap-northeast-2	ap-northeast-2
Asie-Pacifique (Singapour)	ap-southeast-1	ap-southeast-1
Asie-Pacifique (Sydney)	ap-southeast-2	ap-southeast-2
Europe (Francfort)	eu-central-1	eu-central-1
Europe (Irlande)	eu-west-1	eu-west-1
Europe (Londres)	eu-west-2	eu-west-2
Afrique (Le Cap)	af-south-1	eu-west-1 eu-west-2
Asie-Pacifique (Hong Kong)	ap-east-1	ap-northeast-1 ap-northeast-2

> **Note**
>
> Les métriques relatives aux clusters Amazon EKS situés à af-south-1, en Afrique (Le Cap) et à ap-east-1, en Asie-Pacifique (Hong Kong) sont exportées vers le service de surveillance AMS dans le même format, respectivement. Région AWS Les métriques correspondantes Régions AWS sont ensuite transportées au sein du service de surveillance AMS vers différentes régions où elles sont traitées et stockées. Consultez le tableau précédent pour les régions que le service de surveillance AMS utilise pour stocker les métriques.

Intégrez la surveillance et la gestion des incidents pour Amazon EKS dans AMS Accelerate

Procédez comme suit pour intégrer la surveillance et la gestion des incidents pour Amazon EKS.

1. Activez les balises d'optimisation des coûts Amazon EKS : consultez la section Marquage de vos ressources pour la facturation dans le guide de l'utilisateur Amazon EKS.
2. Initiez l'intégration de la surveillance et de la gestion des incidents pour EKS : contactez votre responsable de prestation de services cloud (CSDM) avec les noms de compte IDs et de cluster pour l'intégrer.
3. Valider les exigences : votre architecte cloud (CA) vérifie que toutes les exigences sont satisfaites avant le début de l'intégration.
4. Mettre à jour le contrôle d'accès basé sur les rôles (RBAC) de Kubernetes : AMS partage les commandes pour implémenter ces modifications. `eksctl` Vous pouvez passer en revue ces modifications, puis les déployer. Vous devez déployer les mises à jour RBAC afin qu'AMS soit autorisé à exécuter des commandes en votre nom. Ces mises à jour incluent le mappage du rôle AMS IAM à un utilisateur Kubernetes, la création d'un nouveau rôle de cluster Kubernetes pour AMS et la liaison du rôle de cluster AMS Kubernetes à l'utilisateur.
5. Déployer les composants du cluster : AMS déploie les composants suivants dans un espace de noms géré par AMS sur votre cluster :
   - Serveur Prometheus
   - Exportateur de nœuds Prometheus (non applicable pour) AWS Fargate
   - kube-state-metrics

6. Effectuer des mises à jour de configuration de Prometheus : AMS configure Prometheus pour permettre l'écriture à distance des métriques.
7. (Facultatif) Configurer les tableaux de bord : votre autorité de certification vous aide à configurer les tableaux de bord Amazon Managed Grafana dans votre compte.

> **Note**
>
> Une fois votre cluster Amazon EKS intégré, AMS analyse les signaux d'alerte et effectue une évaluation de base pour identifier les problèmes existants dans votre cluster. Une fois l'évaluation de base terminée, AMS partage les résultats et les recommandations de résolution par le biais de Trusted Advisor et d'une demande de service que vous pouvez utiliser pour résoudre les problèmes de votre cluster. À partir de cette évaluation, AMS crée une base de surveillance Amazon EKS spécifique à vos clusters EKS en ajustant nos seuils d'alarme au niveau du compte. Pour éliminer les réponses AMS dupliquées par rapport à ces résultats, nous ajustons notre surveillance pour exclure ces signaux d'alerte. Nous réajustons notre surveillance pour inclure les signaux lorsque votre CSDM nous informe que les problèmes sous-jacents ont été corrigés.

Abandonnez la surveillance et la gestion des incidents pour Amazon EKS dans AMS Accelerate

Informez votre responsable de prestation de services cloud (CSDM) avec les noms de compte IDs et de cluster pour démarrer le processus de délocalisation. Une fois que vous avez quitté le système, le traitement des alertes, le stockage des métriques et les requêtes de métriques sont suspendus et les métriques sont supprimées conformément aux politiques de conservation des données par défaut d'Amazon Managed Service for Prometheus.

AMS effectue les étapes de déchargement suivantes :

1. AMS désactive les alertes qui vous sont envoyées ainsi qu'à AMS Operations.
2. AMS supprime l'instance Prometheus de votre cluster Amazon EKS.
3. AMS supprime les autres AWS ressources installées sur votre compte, telles que les rôles et les AWS Config règles IAM.

Une fois ces étapes terminées, vous devez effectuer les étapes de déchargement suivantes :

1. `eksctl`À utiliser pour supprimer les autorisations RBAC Kubernetes du. `aws-auth` `ConfigMap`
2. Si vous l'avez déjà installée, supprimez l'instance Amazon Managed Grafana que vous avez configurée pour vous connecter à AMS.

Gestion de la continuité dans AMS Accelerate

AMS s'appuie sur AWS Backup la centralisation et l'automatisation de la sauvegarde de vos données dans tous AWS les services. Les plans de sauvegarde AMS fournissent les meilleures pratiques pour différents cas d'utilisation ; vous pouvez toutefois continuer à utiliser vos plans de sauvegarde existants. Une fois que vous avez intégré la gestion des sauvegardes AMS, AMS fournit des rapports de sauvegarde, et les experts d'AMS surveillent en permanence vos tâches de sauvegarde pour s'assurer que vous disposez d'une solution de sauvegarde fiable.

Pour en savoir plus, consultez AWS Backup: Fonctionnement et AWS Ressources prises en charge et applications tierces.

AMS Accelerate fournit une gamme de services opérationnels pour vous aider à atteindre l'excellence opérationnelle sur AWS. Pour comprendre rapidement comment AMS aide vos équipes à atteindre l'excellence opérationnelle globale AWS Cloud grâce à certaines de nos principales fonctionnalités opérationnelles, notamment le service d'assistance 24 h/24, 7 j/7, la surveillance proactive, la sécurité, l'application de correctifs, la journalisation et la sauvegarde, consultez les diagrammes d'architecture de référence AMS.

Regardez la vidéo de Carl pour en savoir plus (9:29)

Rubriques

- Comment fonctionne la gestion de la continuité dans AMS
- Sélectionnez un plan de sauvegarde AMS
- Étiquetez vos ressources pour appliquer les plans de sauvegarde AMS
- Afficher les sauvegardes dans les coffres-forts AMS
- Surveillance et génération de rapports sur les sauvegardes AMS

Comment fonctionne la gestion de la continuité dans AMS

Les plans de sauvegarde AMS définissent la fréquence de sauvegarde de vos données et la politique de conservation de vos sauvegardes. Les coffres-forts de sauvegarde AMS permettent d'organiser vos données de sauvegarde. Une fois qu'une ressource est associée à un plan de sauvegarde, les ressources compatibles sont sauvegardées de manière incrémentielle. La première sauvegarde est une copie complète et les sauvegardes suivantes capturent les modifications incrémentielles. En

fonction de la ressource et du plan de sauvegarde AMS sélectionnés, la Point-in-time restauration (PITR) vous permet de revenir en arrière en sélectionnant l'heure de votre restauration. Pour commencer à utiliser AMS Backup Management, il vous suffit de sélectionner un plan de sauvegarde AMS et de baliser vos ressources.

> **Note**
>
> Assurez-vous que cette option AWS Backup est activée pour chaque compte et chaque type de ressource en suivant les étapes ci-dessous : Mise en route 1 : Inscription au service. Région AWS
> Il n'est pas nécessaire de passer à la section Mise en route 2 : Création d'une sauvegarde à la demande.

Sujets connexes de AWS Backup

- Utilisation des sauvegardes (création, modification, copie, restauration, suppression)
- Création d'une sauvegarde à la demande
- Création de copies de sauvegarde sur Régions AWS
- AWS Backup Services pris en charge
- Point-in-time restaurer
- AWS Backup Fonctions

Sélectionnez un plan de sauvegarde AMS

AMS propose trois plans de sauvegarde différents avec un quatrième plan de sauvegarde afin de minimiser les coûts lors de l'intégration. Pour sélectionner un plan de sauvegarde AMS pour chaque ressource prise en charge, balisez la ressource avec le tag associé au plan. Lors de votre intégration à Accelerate, AMS travaillera avec vous pour identifier le plan de sauvegarde le mieux adapté à vos besoins.

> **Important**
>
> Ne modifiez pas vos plans de sauvegarde AMS par défaut car vos modifications risquent d'être perdues. Créez plutôt de nouveaux plans pour vos configurations personnalisées. Pour plus d'informations, consultez la section Création d'un plan de sauvegarde.

Plan de sauvegarde AMS par défaut

AWS Backup la sauvegarde continue n'est pas activée pour ce plan de sauvegarde ; pour plus de détails, voir Restauration à une heure spécifiée à l'aide de la point-in-time restauration (PITR).

Clé TAG : `ams:rt:backup-orchestrator`

Valeur TAG : `true`

Plan de sauvegarde AMS par défaut	Start Time	Retention
sauvegarde horaire	N/A	N/A
sauvegarde quotidienne	tous les jours à 4:00 UTC	7 jours
sauvegarde hebdomadaire	Samedi, 2h00 UTC	4 semaines
sauvegarde mensuelle	1er du mois, 2h00 UTC	26 semaines
sauvegarde annuelle	1er janvier, 14h00 UTC	2 ans

Plan de sauvegarde amélioré

AWS Backup la sauvegarde continue est activée avec une rétention maximale (31 jours) sur les ressources prises en charge ; pour plus de détails, voir Restauration à une heure spécifiée à l'aide de la point-in-time restauration (PITR) et Services et applications pris en charge pour la point-in-time restauration (PITR).

Clé TAG : `ams:rt:backup-orchestrator-enhanced`

Valeur TAG : `true`

Plan de sauvegarde amélioré	Start Time	Retention
sauvegarde horaire	N/A	N/A
sauvegarde quotidienne	tous les jours à 4:00 UTC	31 jours

Plan de sauvegarde amélioré	Start Time	Retention
sauvegarde hebdomadaire	Samedi, 2h00 UTC	6 semaines
sauvegarde mensuelle	1er du mois, 2h00 UTC	26 semaines
sauvegarde annuelle	1er janvier, 14h00 UTC	2 ans

Plan de sauvegarde sensible aux données

AWS Backup la sauvegarde continue est activée avec une rétention maximale (31 jours) sur les ressources prises en charge ; pour plus de détails, voir Restauration à une heure spécifiée à l'aide de la point-in-time restauration (PITR) et Services et applications pris en charge pour la point-in-time restauration (PITR).

Clé TAG : `ams:rt:backup-orchestrator-data-sensitive`

Valeur TAG : `true`

Plan de sauvegarde sensible aux données	Start Time	Retention
sauvegarde horaire	toutes les heures	7 jours
sauvegarde quotidienne	tous les jours à 4:00 UTC	31 jours
sauvegarde hebdomadaire	Samedi, 2h00 UTC	6 semaines
sauvegarde mensuelle	1er du mois, 2h00 UTC	26 semaines
sauvegarde annuelle	1er janvier, 14h00 UTC	2 ans

Plan de sauvegarde pour l'intégration d'AMS Accelerate

AWS Backup la sauvegarde continue n'est pas activée pour ce plan de sauvegarde ; pour plus de détails, voir Restauration à une heure spécifiée à l'aide de la point-in-time restauration (PITR).

Clé TAG : `ams:rt:backup-orchestrator-onboarding`

Valeur TAG : `true`

Plan de sauvegarde pour l'intégration d'AMS Accelerate	Start Time	Retention
sauvegarde horaire	toutes les heures	2 semaines
sauvegarde quotidienne	N/A	N/A
sauvegarde hebdomadaire	N/A	N/A
sauvegarde mensuelle	N/A	N/A
sauvegarde annuelle	N/A	N/A

AWS Backup Sujets connexes

- Création d'un plan de sauvegarde
- Point-in-time restore (PITR) permet des sauvegardes continues des ressources prises en charge et vous permet de sélectionner une heure précise pour votre restauration. Pour obtenir la liste des ressources prises en charge, voir Disponibilité des fonctionnalités par ressource.

Étiquetez vos ressources pour appliquer les plans de sauvegarde AMS

Pour attribuer des ressources à un plan de sauvegarde AMS, balisez la ressource avec la paire clé-valeur tag du plan. Vous pouvez utiliser AMS Resource Tagger pour appliquer les plans de sauvegarde AMS à un sous-ensemble de vos ressources ou à toutes les ressources prises en charge dans votre compte. Si vous souhaitez utiliser une autre méthode pour appliquer des balises à vos ressources, comme AWS CloudFormation ou Terraform, désactivez Resource Tagger afin qu'il n'entre pas en concurrence avec la méthode de balisage que vous avez choisie. Pour de plus amples informations, veuillez consulter Empêcher le Resource Tagger de modifier les ressources.

L'exemple suivant montre comment utiliser Resource Tagger pour appliquer le plan de sauvegarde AMS par défaut aux instances Amazon Elastic Compute Cloud de votre compte. Pour ce plan de sauvegarde, appliquez la clé `ams:rt:backup-orchestrator` et la valeur du tag`true`. Pour utiliser un autre plan de sauvegarde, modifiez la clé pour qu'elle corresponde à la clé de balise du plan

de sauvegarde souhaité. Pour en savoir plus sur AMS Resource Tagger et comprendre comment intégrer le profil référencé suivant au profil actuel (déjà configuré) de votre compte Accelerate, consultezAccélérez Resource Tagger.

1. Ouvrez la AWS AppConfig console sur https://console.aws.amazon.com/systems-manager/appconfig.
2. Choisissez l'application ResourceTagger.
3. Choisissez l'onglet Profils de configuration, puis choisissez CustomerManagedTags
4. Choisissez Créer pour créer une nouvelle version.
5. Choisissez JSON, puis copiez-collez l'objet JSON suivant :

```
{
    "AWS::EC2::Instance": {
        "AccelerateBackupPlan": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "*"
                    }
                ]
            },
            "Tags": [
                {
                    "Key": "ams:rt:backup-orchestrator",
                    "Value": "true"
                }
            ]
        }
    }
}
```

6. Choisissez Créer une version de configuration hébergée.
7. Choisissez Démarrer le déploiement.
8. Définissez les détails de déploiement suivants :

```
Environment: AMSInfrastructure
Hosted configuration version: Select the version that you have just created.
Deployment Strategy: AMSNoBakeDeployment
```

9. Choisissez Démarrer le déploiement. Resource Tagger balise vos instances`ams:rt:backup-orchestrator: true`, garantissant ainsi qu'elles sont sauvegardées conformément au plan de sauvegarde AMS par défaut.

Afficher les sauvegardes dans les coffres-forts AMS

Vous pouvez contrôler les notifications du coffre-fort de sauvegarde au niveau de chaque coffre-fort à l'aide de balises. Vous pouvez désactiver les notifications pour un coffre-fort spécifique en ajoutant la balise `AMSNotificationOptOut` et en définissant la valeur `True` sur un coffre-fort spécifique. Pour continuer à recevoir des notifications depuis le coffre-fort, supprimez le tag.

Pour afficher la liste de vos sauvegardes AMS, ouvrez la AWS Backup console. Dans le volet de navigation, choisissez Backup vaults et sélectionnez l'un des coffres-forts de sauvegarde AMS dans les tableaux suivants. Dans la section Sauvegardes, consultez la liste de toutes les sauvegardes du coffre de sauvegarde. Sélectionnez une sauvegarde à modifier, supprimer ou restaurer.

Coffres-forts pour les plans de sauvegarde AMS

Nom du coffre-fort AMS	Clé de balise du plan de sauvegarde AMS
ams-automated-backups	ams:rt:backup-orchestrator
ams-automated-enhanced-backups	ams : rt : backup-orchestrator-enhanced
ams-automated-data-sensitive-sauvegardes	ams : rt : backup-orchestrator-data-sensitive
ams-onboarding-backups	ams : rt : backup-orchestrator-onboarding

Autres coffres-forts AMS

Nom du coffre-fort AMS	Description
ams-manual-backups	Ce coffre-fort contient des sauvegardes démarrées manuellement créées par le document `AWSManagedServices-StartBackupJob` SSM Automation et des sauvegardes préalables aux correctifs créées

Nom du coffre-fort AMS	Description
	par les automatisations de correctifs AMS avant l'application des correctifs.
ams-custom-backups	Il s'agit du coffre recommandé pour les sauvegardes créées en dehors des plans de sauvegarde AMS.

AWS Backup Sujets connexes

- Afficher les sauvegardes par ressource
- Utilisation des sauvegardes

Surveillance et génération de rapports sur les sauvegardes AMS

> **Important**
>
> La surveillance et le reporting des sauvegardes AMS ne sont disponibles que dans les régions prises en charge par AMS. Il s'agit des États-Unis Est (Virginie), de l'Ouest (Californie du Nord), de l'Ouest (Oregon), de l'Est des États-Unis (Ohio), du Canada (Centre), de l'Amérique du Sud (São Paulo), de l'UE (Francfort), de l'UE (Londres), de l'UE (Paris), de l'Asie-Pacifique (Mumbai), de l'Asie-Pacifique (Séoul), de l'Asie-Pacifique (Singapour), de l'Asie-Pacifique (Sydney) et de l'Asie-Pacifique (Tokyo).

AMS génère des rapports quotidiens en libre-service ainsi que des rapports mensuels sur la couverture des ressources et l'état des tâches de sauvegarde. Les rapports mensuels sont partagés dans Monthly Business Reviews (MBRs). Pour en savoir plus sur les rapports de sauvegarde quotidiens, voir Rapport de sauvegarde quotidien Rapport .

Les experts AMS surveillent toutes vos tâches de sauvegarde configurées à l'aide de AWS Backup. En cas d'échec de sauvegarde, AMS enquête sur l'échec et vous en informe en vous indiquant la cause première et les options de correction, le cas échéant. Pour éviter le bruit des alertes, lors d'événements entraînant un nombre élevé de défaillances de sauvegarde dans vos comptes, AMS émet une recommandation collective, par le biais de votre CSDM, au lieu de vous avertir pour chaque échec individuel.

Notez qu'AMS ne surveille aucune sauvegarde configurée à l'aide de la fonctionnalité de sauvegarde autonome d'un AWS service.

Comprendre la gestion des correctifs dans AMS Accelerate

> **Important**
>
> Accelerate Patch reporting déploie régulièrement une politique basée sur les AWS Glue ressources. Sachez que les mises à jour du système de correctifs AMS remplacent les politiques basées sur les AWS Glue ressources existantes.

> **Important**
>
> Vous pouvez spécifier d'autres référentiels de correctifs pour les nœuds gérés. Pendant qu'AMS implémente les configurations de correctifs que vous avez demandées, vous êtes responsable de la sélection et de la validation de la sécurité des référentiels que vous avez choisis. Vous devez également accepter tous les risques liés à l'utilisation de ces référentiels, tels que les risques liés à la chaîne d'approvisionnement.
> Les meilleures pratiques pour la sécurité de votre processus de gestion des correctifs sont les suivantes :
>
> - Utilisez uniquement des sources de référentiel fiables et vérifiées
> - Utilisez par défaut les référentiels des fournisseurs de systèmes d'exploitation standard lorsque cela est possible
> - Auditez régulièrement les configurations de référentiels personnalisées

Vous pouvez utiliser le système de correctifs AMS Accelerate, Patch Add-On, pour appliquer des correctifs à vos instances avec des mises à jour liées à la sécurité et d'autres types de mises à jour. Le module complémentaire Accelerate Patch est une fonctionnalité qui fournit des correctifs basés sur des balises pour les instances AMS. Il tire parti des fonctionnalités AWS Systems Manager (SSM) qui vous permettent de baliser les instances et de leur faire appliquer des correctifs à l'aide d'une ligne de base et d'une fenêtre que vous configurez. Le module complémentaire AMS Accelerate Patch est une option d'intégration. Si vous ne l'avez pas obtenu lors de l'intégration de votre compte Accelerate, contactez votre responsable de prestation de services cloud (CSDM) pour l'obtenir.

La gestion des correctifs AMS Accelerate utilise la fonctionnalité de base de correctifs de Systems Manager pour contrôler la définition des correctifs appliqués à une instance. La ligne de base

des correctifs contient la liste des correctifs préapprouvés ; par exemple, tous les correctifs de sécurité. La conformité de l'instance est mesurée par rapport à la ligne de base du correctif qui lui est associée. AMS Accelerate installe par défaut tous les correctifs disponibles pour maintenir l'instance à jour.

> **Note**
>
> AMS Accelerate applique uniquement les correctifs du système d'exploitation (OS). Par exemple, pour Windows, seules les mises à jour Windows sont appliquées, pas les mises à jour Microsoft.

Pour plus d'informations sur les rapports, voirRapports de gestion des hôtes AMS.

AMS Accelerate fournit une gamme de services opérationnels pour vous aider à atteindre l'excellence opérationnelle sur AWS. Pour comprendre rapidement comment AMS aide vos équipes à atteindre l'excellence opérationnelle globale AWS Cloud grâce à certaines de nos principales fonctionnalités opérationnelles, notamment le service d'assistance 24 h/24, 7 j/7, la surveillance proactive, la sécurité, l'application de correctifs, la journalisation et la sauvegarde, consultez les diagrammes d'architecture de référence AMS.

Rubriques

- Recommandations relatives aux correctifs
- Création d'une fenêtre de maintenance des correctifs dans AMS
- Patch avec crochets
- Base de référence des correctifs AMS Accelerate
- Création d'un rôle IAM pour l'application de correctifs à la demande à AMS Accelerate
- Comprendre les notifications relatives aux correctifs et les défaillances des correctifs dans AMS Accelerate

Recommandations relatives aux correctifs

Si vous êtes impliqué dans des opérations d'applications ou d'infrastructures, vous comprenez l'importance d'une solution de correction du système d'exploitation (OS) suffisamment flexible et évolutive pour répondre aux diverses exigences de vos équipes d'application. Dans une organisation

classique, certaines équipes d'application utilisent une architecture qui implique des instances immuables, tandis que d'autres déploient leurs applications sur des instances mutables.

Pour plus d'informations sur les directives AWS prescriptives relatives à l'application de correctifs, consultez la section Application automatique de correctifs pour les instances mutables dans le cloud hybride à l'aide de AWS Systems Manager

> **Note**
>
> Le module complémentaire Accelerate Patch est une fonctionnalité qui fournit des correctifs basés sur des balises pour les instances AMS. Il tire parti des fonctionnalités AWS Systems Manager (SSM) qui vous permettent de baliser les instances et de leur faire appliquer des correctifs à l'aide d'une ligne de base et d'une fenêtre que vous configurez. Le module complémentaire AMS Accelerate Patch est une option d'intégration. Si vous ne l'avez pas obtenu lors de l'intégration de votre compte Accelerate, contactez votre responsable de prestation de services cloud (CSDM) pour l'obtenir.

Recommandations relatives à la responsabilité des correctifs

Le processus d'application des correctifs pour les instances persistantes doit impliquer les équipes et les actions suivantes :

- Les équipes chargées des applications (DevOps) définissent les groupes de correctifs pour leurs serveurs en fonction de l'environnement de l'application, du type de système d'exploitation ou d'autres critères. Ils définissent également les fenêtres de maintenance spécifiques à chaque groupe de correctifs. Ces informations doivent être stockées sur des balises associées aux instances. Les noms de balises recommandés sont « Patch Group » et « Maintenance Window ». Au cours de chaque cycle de correctifs, les équipes chargées des applications se préparent à appliquer les correctifs, testent l'application après l'application et résolvent les éventuels problèmes liés à leurs applications et à leur système d'exploitation pendant l'application des correctifs.
- L'équipe chargée des opérations de sécurité définit les lignes de base des correctifs pour les différents types de systèmes d'exploitation utilisés par les équipes chargées des applications et met les correctifs à disposition via le gestionnaire de correctifs de Systems Manager.
- La solution d'application automatique des correctifs s'exécute régulièrement et déploie les correctifs définis dans les lignes de base des correctifs, en fonction des groupes de correctifs et des fenêtres de maintenance définis par l'utilisateur.

- Les équipes de gouvernance et de conformité définissent les directives relatives aux correctifs ainsi que les processus et mécanismes d'exception.

Pour plus d'informations, consultez la section Conception de solutions de correctifs pour les instances mutables. EC2

Conseils pour les équipes de candidature

- Passez en revue et familiarisez-vous avec la création et la gestion des fenêtres de maintenance ; voir Fenêtres de AWS Systems Manager maintenance et Création d'une fenêtre de maintenance SSM pour l'application de correctifs pour en savoir plus. La compréhension de la structure générale et de l'utilisation des fenêtres de maintenance vous permet de comprendre les informations à fournir si vous n'êtes pas la personne qui les crée.
- Pour les configurations de haute disponibilité (HA), prévoyez une fenêtre de maintenance par zone de disponibilité et par environnement (Dev/Test/Prod). Cela garantira une disponibilité continue pendant l'application des correctifs.
- La durée de la fenêtre de maintenance recommandée est de 4 heures avec une limite d'une heure, plus 1 heure supplémentaire pour 50 instances
- Les versions de développement et de test des correctifs sont espacées de suffisamment de temps pour vous permettre d'identifier les problèmes potentiels avant d'appliquer les correctifs de production.
- Automatisez les tâches courantes avant et après l'application des correctifs via l'automatisation SSM et exécutez-les en tant que tâches de maintenance. Notez que pour les tâches postérieures à l'application des correctifs, vous devez vous assurer que le temps imparti est suffisant, car les tâches ne seront pas lancées une fois la date limite atteinte.
- Familiarisez-vous avec les lignes de base des correctifs et leurs fonctionnalités, notamment en ce qui concerne les délais d'approbation automatique pour les types de gravité des correctifs, qui peuvent être utilisés pour garantir que seuls les correctifs appliqués seront appliqués en production à Dev/Test une date ultérieure. Consultez la section À propos des lignes de base des correctifs pour plus de détails.

Conseils pour les équipes chargées des opérations de sécurité

- Passez en revue les lignes de base des correctifs et familiarisez-vous avec celles-ci. L'approbation des correctifs est gérée de manière automatisée et comporte différentes options de règles. Pour plus d'informations, reportez-vous à la section À propos des lignes de base des correctifs.
- Discutez des besoins en matière d'application de correctifs Dev/Test/Prod avec les équipes chargées des applications et développez plusieurs bases de référence pour répondre à ces besoins.

Conseils pour les équipes de gouvernance et de conformité

- L'application de correctifs doit être une fonction « Opt Out ». Une fenêtre de maintenance par défaut et un balisage automatique doivent exister pour garantir que rien ne reste sans correctif. AMS Resource Tagger peut vous y aider ; discutez de cette option avec votre architecte cloud (CA) ou votre responsable de prestation de services cloud (CSDM) pour obtenir des conseils sur la mise en œuvre.
- Les demandes d'exemption de l'application de correctifs doivent nécessiter une documentation justifiant l'exemption. Un responsable de la sécurité informatique (CISO) ou un autre responsable de l'approbation doit approuver ou refuser la demande.
- La conformité des correctifs doit être contrôlée régulièrement via la console Patch Manager, Security Hub ou un scanner de vulnérabilités.

Exemple de conception pour une application Windows à haute disponibilité

Vue d'ensemble :

- Une fenêtre de maintenance par AZ.
- Un ensemble de fenêtres de maintenance par environnement.
- Une ligne de base de correctifs par environnement :
  - Dev : Approuver toute la sévérité et la classification après 0 jour.
  - Test : Approuvez les correctifs de mise à jour de sécurité critiques après 0 jour et toutes les autres classifications et niveaux de gravité après 7 jours.

- Prod : Approuvez les correctifs de mise à jour de sécurité critiques après 0 jour et toutes les autres classifications et niveaux de gravité après 14 jours.

CloudFormation Scripts :

Ces scripts sont configurés pour créer les fenêtres de maintenance, les lignes de base et les tâches de correction pour une EC2 application Windows HA à deux zones de disponibilité à l'aide des paramètres d'approbation de base décrits ci-dessus.

- Exemple de pile CFN pour Windows Dev : HA-Patching-Dev-Stack.json
- Exemple de pile CFN pour Windows : HA-Patching-Test-Stack.json
- Exemple de pile CFN pour Windows Prod : HA-Patching-Prod-Stack.json

Recommandations relatives aux correctifs FAQs

Q : Comment puis-je gérer les correctifs imprévus pour les exploits « 0 » jours ?

R : SSM prend en charge une fonctionnalité Patch Now qui utilise la ligne de base par défaut actuelle pour le système d'exploitation de l'instance. AMS déploie un ensemble par défaut de lignes de base de correctifs qui approuve tous les correctifs au bout de 0 jour. Toutefois, lors de l'utilisation de la fonctionnalité Patch Now, aucun instantané préalable au correctif n'est pris, car cette commande exécute le document RunPatchBaseline AWS-SSM. Nous vous recommandons d'effectuer une sauvegarde manuelle avant de procéder à l'application des correctifs.

Q : AMS prend-il en charge l'application de correctifs pour les instances dans Auto-Scaling Groups () ? ASGs

R : Non À l'heure actuelle, les correctifs ASG ne sont pas pris en charge pour les clients Accelerate.

Q : Y a-t-il des limites à prendre en compte dans Maintenance Windows ?

R : Oui, il y a quelques limites dont vous devez être conscient.

- Fenêtres de maintenance par compte : 50
- Tâches par fenêtre de maintenance : 20
- Nombre maximum d'automatisations simultanées par fenêtre de maintenance : 20
- Nombre maximum de fenêtres de maintenance simultanées : 5

Pour une liste complète des limites SSM par défaut, consultez la section AWS Systems Manager Points de terminaison et quotas.

Création d'une fenêtre de maintenance des correctifs dans AMS

Une fenêtre de maintenance des correctifs exécute les automatisations des correctifs AMS selon un calendrier défini pour les EC2 instances Amazon ciblées. Les cibles sont définies par une ou plusieurs balises pour un groupe d'instances. Vous pouvez définir des horaires en fonction des jours et des heures autour du Patch Tuesday, ou vous pouvez définir un calendrier à l'aide d'une expression cron. Pour plus d'informations, reportez-vous à la section Reference : Cron and rate expressions for Systems Manager dans le guide de l'AWS Systems Manager utilisateur. Avant d'appliquer le correctif, AMS crée un instantané du volume racine de chaque instance. Si AMS détecte que l'application de correctifs a un impact sur l'état de santé de l'instance, ou si vous informez AMS de l'impact de l'application de correctifs, AMS utilise cet instantané pour restaurer le volume racine à un état antérieur au correctif.

Limites des fenêtres de maintenance des correctifs AMS Accelerate

Utilisations des correctifs AMS AWS Systems Manager (Systems Manager). Outre les limites du service Systems Manager, l'application de correctifs AMS est limitée à 300 instances cibles par fenêtre de maintenance des correctifs. Étant donné que le délai d'exécution des correctifs est généralement de 30 minutes par instance, le tableau suivant fournit des exemples du nombre de fenêtres et de durées de maintenance.

Instances à patcher	Durée des fenêtres de maintenance (heures)	Fenêtres de maintenance simultanées nécessaires
100	1	1
200	1	1
300	2	1
600	3	2
800	4	3
1200	6	4

Instances à patcher	Durée des fenêtres de maintenance (heures)	Fenêtres de maintenance simultanées nécessaires
1 500	8	5

> **Important**
>
> Ces exemples supposent qu'aucune autre fenêtre de maintenance de Systems Manager n'est active et qu'aucune autre automatisation n'est en cours d'exécution.

Pour plus d'informations sur les limites, consultez la section AWS Systems Manager Points de terminaison et quotas.

Rubriques

- Créez une fenêtre de maintenance récurrente « Patch Tuesday » depuis la console AMS (recommandé)
- Créez une fenêtre de maintenance des correctifs à l'aide AWS CloudFormation d'AMS Accelerate
- Création d'une fenêtre de maintenance depuis la console Systems Manager pour AMS Accelerate
- Créez une fenêtre de maintenance avec l'interface de ligne de commande (CLI) de Systems Manager pour AMS Accelerate

Créez une fenêtre de maintenance récurrente « Patch Tuesday » depuis la console AMS (recommandé)

Microsoft publie des correctifs pour ses systèmes d'exploitation le deuxième mardi de chaque mois, également connu sous le nom de Patch Tuesday. Il est courant de planifier l'application de correctifs pour les instances Windows et Linux par rapport au Patch Tuesday. Pour planifier des fenêtres de maintenance des correctifs récurrentes le premier ou le deuxième week-end après le Patch Tuesday, rendez-vous sur la console AMS et procédez comme suit :

1. Donnez un nom à votre fenêtre de maintenance des correctifs.
2. [facultatif] Fournissez une description de la fenêtre de maintenance des correctifs.
3. Sélectionnez un jour par rapport au Patch Tuesday.

4. Entrez l'heure de début de la fenêtre de maintenance des correctifs dans hh:mm. Par exemple, minuit est minuit et 23 h 00. Sélectionnez ensuite un fuseau horaire.
5. [facultatif] Modifiez la durée en fonction de vos besoins. AMS recommande une durée minimale de quatre heures.
6. Entrez une clé de balise de patch et une valeur pour la cible. Pour plus d'informations, voir Que sont les tags ? .
7. [facultatif] Développez les paramètres facultatifs pour ajuster la simultanéité, le taux d'erreur et la limite de la fenêtre de maintenance.

    1. La simultanéité contrôle le nombre d'instances cibles auxquelles des correctifs sont appliqués en même temps. Par exemple, une simultanéité de 50 % pour 10 instances cibles ne corrigera pas plus de 5 instances à la fois, tandis qu'une simultanéité de 100 % corrigera les 10 instances en même temps.
    2. Le taux d'erreur contrôle la tolérance aux erreurs avant la suspension de l'application des correctifs. Par exemple, un taux d'erreur de 100 % pour 10 instances cibles corrigera toutes les instances, quel que soit le nombre d'instances défaillantes, tandis qu'un taux d'erreur de 50 % suspendra l'application des correctifs une fois que 5 instances n'auront pas été corrigées. AMS recommande un taux d'erreur de 100 %.
    3. La fermeture de la fenêtre de maintenance des correctifs empêche toute violation de la fenêtre de maintenance des correctifs en suspendant le début des nouvelles activités d'application des correctifs les heures spécifiées avant la fin de la fenêtre de maintenance des correctifs. Par exemple, un délai d'une heure (recommandé) met fin à l'activité des nouveaux correctifs 1 heure avant la fin de la fenêtre de maintenance des correctifs.

> **Important**
>
> Vérifiez l'heure de la prochaine exécution.
> Accédez à la console de la fenêtre de maintenance SSM, recherchez la fenêtre de maintenance des correctifs que vous venez de créer et vérifiez l'heure de la prochaine exécution. Si vous avez des questions ou si vous devez modifier votre fenêtre de maintenance des correctifs, créez une demande de service pour parler à un expert des correctifs AMS

Pour planifier une fenêtre de maintenance des correctifs basée sur Cron à l'aide CloudFormation de. Créez une fenêtre de maintenance des correctifs à l'aide AWS CloudFormation d'AMS Accelerate

Créez une fenêtre de maintenance des correctifs à l'aide AWS CloudFormation d'AMS Accelerate

Pour créer une fenêtre de maintenance des correctifs AMS Accelerate à l'aide de AWS CloudFormation, connectez-vous d'abord à votre compte Accelerate et sélectionnez l' Région AWS emplacement de vos instances cibles. Suivez ensuite ces étapes sur le fichier https://console.aws.amazon.com/cloudformation :

1. Sélectionnez l'un des deux CloudFormation modèles de correctifs Accelerate personnalisés.

   - Planification du mardi des correctifs : Microsoft publie des correctifs pour ses systèmes d'exploitation le deuxième mardi de chaque mois, également appelé mardi des correctifs, afin de planifier les fenêtres de maintenance des correctifs le premier ou le deuxième week-end suivant le mardi des correctifs : une fois connecté à la console Accelerate, utilisez ce PatchTuesdayScheduling CloudFormation modèle de lien.
   - Planification CRON : pour créer des fenêtres de maintenance des correctifs à l'aide de CRON afin de définir le jour de début, utilisez ce modèle de lien CRONScheduling CloudFormation . N'oubliez pas que Systems Manager CRON compte les jours 1 à 7 (pour plus de détails sur Systems Manager CRON, voir Reference : Cron and rate expressions for Systems Manager).

   Le choix de l'un de ces liens entraîne le chargement automatique du modèle sur la CloudFormation console. Ensuite, cliquez sur Suivant.
2. Sur la page Spécifier les détails de la pile (étape 2 des pages Créer une pile), entrez le nom de la pile et les paramètres du modèle (les paramètres par défaut affichés sont ceux recommandés par AMS, sélectionnez le jour et les heures correspondant à votre cas d'utilisation). Cliquez ensuite sur Suivant.
3. Configurez les options de pile (facultatif). Pour plus d'informations sur les options, consultez la section Configuration des options de CloudFormation pile AWS. Cliquez ensuite sur Suivant.
4. Vérifiez les valeurs de votre pile (facultatif). Pour plus d'informations sur l'examen des détails de la pile afin d'estimer les coûts, voir Révision de votre pile et estimation du coût de la pile. Lorsque vous êtes prêt, cliquez sur Créer une pile.

   La création de la pile peut prendre jusqu'à une minute. Une fois la pile créée avec succès, votre fenêtre de maintenance des correctifs s'exécute à l'heure spécifiée. Vous pouvez apporter des modifications à votre fenêtre de maintenance des correctifs en créant et en exécutant un ensemble de CloudFormation modifications (recommandé) (pour plus de détails, voir Création

de piles à l'aide d'ensembles de modifications) ou en mettant à jour la fenêtre de maintenance des correctifs sur la console de la fenêtre de maintenance de Systems Manager (). https://console.aws.amazon.com/systems-manager/maintenance-windows

Regardez la vidéo de Namrata pour en savoir plus (5:41)

Création d'une fenêtre de maintenance depuis la console Systems Manager pour AMS Accelerate

Pour créer une fenêtre de maintenance AMS Accelerate depuis la console Systems Manager, procédez comme suit :

1. Dans la barre de navigation de gauche de la zone Gestion des modifications, cliquez sur Fenêtres de maintenance, puis sur Créer une fenêtre de maintenance en haut à droite de l'écran. Remplissez le formulaire. Pour plus de détails sur les options, voir Créer une fenêtre de maintenance (console). Lorsque vous avez terminé, cliquez sur Créer une fenêtre de maintenance.

   La page de liste des fenêtres de maintenance s'ouvre.
2. Sélectionnez la fenêtre de maintenance nouvellement créée.

   La page de détails de la fenêtre de maintenance s'ouvre.
3. Accédez à l'onglet Cibles et choisissez Enregistrer la cible.

   La page cible Enregistrer s'ouvre.
4. Ajoutez votre objectif Accelerate. Pour plus d'informations sur les cibles, voir Affecter des cibles à une fenêtre de maintenance (console). Lorsque vous avez terminé, cliquez sur Enregistrer la cible. Prenez note de la cible lorsque vous en aurez besoin plus tard.

   La page de détails des fenêtres de maintenance s'ouvre à nouveau dans l'onglet Cibles avec une liste incluant la nouvelle cible.
5. Dans l'onglet Tâches de la page de détails de la fenêtre de maintenance, choisissez Enregistrer la tâche, puis sélectionnez Enregistrer la tâche d'automatisation dans la liste déroulante. Remplissez le formulaire. Accélérez les notes :

   - Donnez un nom de tâche significatif. Par exemple : AcceleratePatch.

- Dans la zone du document Automation, cliquez dans le champ de recherche, choisissez Propriétaire, puis Documents partagés.
- Sélectionnez le document d'automatisation en cliquant dans la zone de recherche et en choisissant Préfixe du nom du document --> Égal, puis en tapant : AWSManagedServices-PatchInstance. Sélectionnez ensuite le AWSManagedServices-PatchInstancedocument en sélectionnant son bouton radio.
- Sous Version du document, sélectionnez Version par défaut au moment de l'exécution.
- Dans la section Cibles :
  - Définissez la cible en : pour sélectionner les groupes cibles enregistrés.
  - Dans la liste des cibles, sélectionnez la cible que vous avez enregistrée dans l'onglet Cibles.
- Dans la section Paramètres d'entrée, remplissez le formulaire.
  - InstanceId: `{{TARGET_ID}}`
  - StartInactiveInstances: `True` pour démarrer les instances si elles sont arrêtées pendant la fenêtre de maintenance des correctifs.

    > **Note**
    >
    > La valeur du InstanceIdparamètre distingue les majuscules et minuscules et la valeur du StartInactiveInstancesparamètre peut être vraie ou fausse.
    > Les instances arrêtées ne peuvent pas être démarrées lorsqu'elles sont ciblées par des balises. Pour plus d'informations, voir Aucune invocation à exécuter.

- Dans la section Contrôle du taux, choisissez des pourcentages. AMS Accelerate recommande 100 % pour la simultanéité et 100 % pour le seuil d'erreur afin de tenter de patcher toutes les instances simultanément, quelles que soient les erreurs d'automatisation. Si vous souhaitez appliquer des correctifs à la moitié de vos cibles à la fois, par exemple, pour maintenir la moitié des instances cibles dans le cadre d'un équilibrage de charge, définissez Concurrency sur 50 %.
- Dans la section Rôle de service IAM, choisissez Utiliser un rôle de service personnalisé, puis choisissez le rôle ams_ssm_automation_role.

Cliquez sur Enregistrer la tâche d'automatisation.

La fenêtre de maintenance des correctifs est créée. Dans l'onglet Description, vous pouvez voir l'heure de la prochaine exécution.

Créez une fenêtre de maintenance avec l'interface de ligne de commande (CLI) de Systems Manager pour AMS Accelerate

Pour créer une fenêtre de maintenance AMS Accelerate à l'aide de l'interface de ligne de commande :

1. Suivez le didacticiel SSM : Créez et configurez une fenêtre de maintenance (AWS CLI). Pour chaque étape du didacticiel, voici des exemples de commandes CLI pour l'application de correctifs.

   > **Note**
   >
   > Ces exemples sont spécifiques à Linux ou macOS. Les commandes peuvent également être exécutées, AWS CloudShell ce qui peut être plus simple que de `awscli` les configurer sur une machine locale. Pour plus de détails, consultez la section Travailler avec AWS CloudShell.

   a. À l'étape 1 du didacticiel, pour créer une fenêtre de maintenance :

   ```
   aws ssm create-maintenance-window \
                   --name Sample-Maintenance-Window \
                   --schedule "cron(0 30 23 ? * TUE#2 *)" \
                   --duration 4 \
                   --cutoff 1 \
                   --allow-unassociated-targets \
                   --tags "Key=Environment,Value=Production"
   ```

   En cas de réussite, `window-id` est renvoyé.

   b. À l'étape 2 du didacticiel, pour enregistrer un nœud cible :

   ```
   aws ssm register-target-with-maintenance-window \
                   --window-id "mw-xxxxxxxxx" \
                   --resource-type "INSTANCE" \
                   --target "Key=tag:Environment,Values=Prod"
   ```

   En cas de réussite, `WindowTargetID` s sont renvoyés.

   c. À l'étape 3 du didacticiel, pour enregistrer une tâche :

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-xxxxxx" \
    --targets "Key=WindowTargetIds,Values=63d4f63c-xxxxxx-9b1d-xxxxxfff" \
    --task-arn "AWSManagedServices-PatchInstance" \
    --service-role-arn "arn:aws:iam::AWS-Account-ID:role/ams_ssm_automation_role"
 \
    --task-invocation-parameters "{\"Automation\":{\"DocumentVersion\":\"\$DEFAULT
\",\"Parameters\":{\"InstanceId\":[\"{{TARGET_ID}}\"],\"StartInactiveInstances\":
[\"True\"]}}}" \
    --max-concurrency 50 \
    --max-errors 50 \
    --name "AutomationExample" \
    --description "Sample Description" \
    --task-type=AUTOMATION
```

Patch avec crochets

Vous pouvez configurer les correctifs AMS pour exécuter des commandes au niveau du système d'exploitation (OS) avant et après l'application des correctifs, à l'aide des patchs AMS. Utilisez les patch-hooks AMS pour exécuter les documents de commande SSM afin d'arrêter un service avant d'appliquer le correctif, puis de le démarrer après l'application du correctif, ou pour exécuter des commandes afin de confirmer que votre application est saine après l'application du correctif.

Pour utiliser les patchhooks AMS, vous devez effectuer les opérations suivantes :

1. Créez des documents de commande SSM à utiliser comme patchhooks.
2. Créez une fenêtre de maintenance des correctifs AMS ou utilisez une fenêtre de maintenance des correctifs AMS existante. Pour plus de détails, consultez la fenêtre de maintenance des correctifs AMS.
3. Configurez une fenêtre de maintenance des correctifs AMS pour utiliser vos documents de commande SSM pour les patchs hooks AMS.

Crochets de raccordement AMS RACI

La matrice responsable, responsable, consultée et informée, ou RACI, attribue la responsabilité principale au client ou à AMS pour diverses activités. Le tableau suivant fournit un aperçu des

responsabilités du client et d'AMS en ce qui concerne les activités d'une application qui utilise des patchhooks AMS.

- R représente la partie responsable qui fait le travail pour accomplir la tâche
- A représente la partie responsable
- C signifie consulté ; partie dont l'opinion est sollicitée, généralement en tant qu'expert en la matière ; et avec laquelle il existe une communication bilatérale
- I signifie informé, c'est-à-dire la partie qui est informée des progrès, souvent uniquement une fois la tâche ou le résultat attendu

Activité	Client	AMS
Création du document de commande pre/post Patch SSM et du contenu du document	R	C
Configurer les paramètres du patch hook pour l'application de correctifs AMS	R	C
Exécuter le pre/post document de commande du correctif SSM	I	R
Triez et répondez aux défaillances des patch-hooks	I	R
Avertir le client de la défaillance du patch hook	I	R
Retour à un état antérieur au correctif si le client le demande	C	R

Création de documents SSM pour les patchhooks

Les patchhooks AMS utilisent les documents Amazon EC2 Systems Manager (SSM) lors de l'application des correctifs. Créez un document de commande SSM ou partagez un document de commande SSM existant avec le compte sur lequel les correctifs ont lieu. Pour plus d'informations sur les documents SSM, y compris les limitations, voir Partage de documents SSM.

Pour créer un document de commande SSM, procédez comme suit :

1. Créez un document SSM avec Type de document = « Commande ».
2. Entrez vos commandes dans la section Contenu. Pour plus d'informations, consultez la section Création du contenu d'un document SSM.

> **Note**
>
> Les documents SSM pour les patch-hooks AMS peuvent également être créés avec AWS CLI ou AWS CloudFormation. Si vous avez besoin d'aide pour créer des documents SSM pour vos patchhooks AMS, contactez votre architecte cloud.

Configurez la fenêtre de maintenance des correctifs AMS pour utiliser vos documents de commande SSM comme patch-hooks AMS

Une fenêtre de maintenance des correctifs AMS est une fenêtre de maintenance de Systems Manager qui exécute l'automatisation des correctifs AMS que vous avez configurée.

Pour modifier une fenêtre de maintenance des correctifs AMS afin d'utiliser des patch-hooks, procédez comme suit :

1. Dans la section https://console.aws.amazon.com/systems-manager/Outils de gestion des modifications dans le volet de navigation de gauche, sélectionnez Maintenance Windows.

   Une page répertoriant les fenêtres de maintenance existantes s'ouvre.
2. Sélectionnez un identifiant de fenêtre commençant par mw-.

   La page de détails de cette fenêtre de maintenance s'ouvre.
3. Sélectionnez l'onglet Tâches et l'ID de tâche de fenêtre avec l'ARN de tâche AMS- PatchInstance et cliquez sur Modifier.

4. Faites défiler la page jusqu'à la section Paramètres et mettez à jour les paramètres suivants.

Paramètres du patch hook AMS :

- PrePatchHook: nom du document SSM de type « Commande » que vous souhaitez exécuter avant d'appliquer le correctif. Laissez ce champ vide ou tapez « AWS-Noop » (en distinguant majuscules et minuscules) si vous n'exécutez pas de commande avant d'appliquer le correctif.
- PostPatchHook: nom du document SSM de type « Commande » que vous souhaitez exécuter après l'application du correctif. Laissez ce champ vide ou tapez « AWS-Noop » (en distinguant majuscules et minuscules) si vous n'exécutez aucune commande après l'application d'un correctif.
- ExecutePatchBasedOnPreHookStatus: Exécutez l'application de correctifs en fonction de la réussite ou de l'échec de l' PrePatchHook exécution, choisissez-en une :
  - OnPreHookSuccess: N'exécutez l'automatisation des correctifs AMS qu'en cas PrePatchHook de réussite.
  - Toujours : exécutez l'automatisation des correctifs AMS en PrePatchHook cas de réussite ou d'échec.
  - OnPreHookFailure- Exécutez l'automatisation des correctifs AMS uniquement en PrePatchHook cas d'échec.
  - Jamais : n'exécutez pas l'automatisation des correctifs AMS. Cela peut être utile lorsque vous testez votre PrePatchHook.
- ExecutePostHookBasedOnPatchStatus: exécutez le hook post-patch en fonction du succès ou de l'échec de l'automatisation des correctifs AMS, choisissez-en un :
  - OnPatchSuccess: N'exécutez le que PostPatchHook lorsque l'automatisation des correctifs AMS s'exécute correctement.
  - Toujours : exécutez le PostPatchHook lorsque l'automatisation des correctifs AMS est réussie et en cas d'échec.
  - OnPatchFailure- Exécutez le PostPatchHook uniquement lorsque l'automatisation des correctifs AMS échoue.

> **Note**
>
> Si la zone de texte de l'une de ces variables est absente, vous pouvez y remédier en faisant défiler la page jusqu'à la section du document d'automatisation, en sélectionnant un autre document, puis en resélectionnant le document d'origine. Cela actualise les paramètres d'entrée afin que vous puissiez les modifier.

Base de référence des correctifs AMS Accelerate

Une référence de correctifs définit les correctifs qui sont approuvés pour l'installation sur vos instances. Vous pouvez spécifier un par un les correctifs approuvés ou rejetés. Vous pouvez également utiliser les règles d'approbation automatique pour spécifier que certains types de mises à jour (par exemple, les mises à jour critiques) doivent être approuvés automatiquement. La liste des mises à jour rejetées remplace à la fois les règles et la liste des mises à jour approuvées.

Ligne de base de correctifs par défaut

Lorsque vous optez pour l'application de correctifs AMS Accelerate, les lignes de base de correctifs par défaut sont remplacées par les lignes de base de correctifs par défaut d'AMS Accelerate pour les systèmes d'exploitation suivants.

- Windows
- Amazon Linux 1
- Amazon Linux 2
- CentOS
- Suse
- Rhel
- Ubuntu

> **Important**
>
> Les lignes de base de correctifs par défaut sont gérées par AMS. Ne modifiez pas les lignes de base des correctifs par défaut, car vos modifications risquent d'être perdues. Créez plutôt

une ligne de base de correctifs personnalisée. Consultez Base de correctifs personnalisée avec AMS Accelerate.

> **Note**
>
> Les lignes de base des correctifs AMS Accelerate définies comme product = * signifient que tous les correctifs sont appliqués à l'instance de toutes les classifications et de toutes les sécurités.

Base de correctifs personnalisée avec AMS Accelerate

Pour utiliser une ligne de base de correctifs personnalisée avec AMS Accelerate, assurez-vous d'abord que vous disposez d'un groupe de correctifs, puis créez la ligne de base personnalisée.

Pour plus d'informations, consultez les ressources suivantes :

- Utilisation de groupes de correctifs
- Création d'une ligne de base de correctifs personnalisée (Windows)
- Création d'une ligne de base de correctifs personnalisée (Linux)
- Mettre à jour ou supprimer une ligne de base de correctifs personnalisée (console)

Création d'un rôle IAM pour l'application de correctifs à la demande à AMS Accelerate

Une fois que votre compte est intégré à AMS Accelerate patching, AMS Accelerate déploie une politique gérée, amspatchmanagedpolicy. Cette politique contient les autorisations requises pour l'application de correctifs à la demande à l'aide du document `AWSManagedServices-PatchInstance` d'automatisation AMS. Pour utiliser ce document d'automatisation, l'administrateur du compte crée un rôle IAM pour les utilisateurs. Procédez comme suit :

Créez un rôle à l'aide de AWS Management Console :

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la.
2. Dans le volet de navigation de la console, choisissez Rôles, puis Créer un rôle.

3. Choisissez un autre type de Compte AWS rôle.
4. Pour ID de compte, entrez l'ID de AWS compte auquel vous souhaitez accorder l'accès à vos ressources.

   L'administrateur du compte spécifié peut accorder l'autorisation d'endosser ce rôle à n'importe quel utilisateur IAM de ce compte. Pour ce faire, l'administrateur attache une politique à l'utilisateur, ou à un groupe, qui accorde l'autorisation d'exécuter l'AssumeRoleaction sts :. Cette politique doit spécifier le nom de ressource Amazon (ARN) du rôle en tant que ressource. Remarques :

   - Si vous accordez des autorisations à des utilisateurs à partir d'un compte que vous ne contrôlez pas et que les utilisateurs assumeront ce rôle par programmation, choisissez Exiger un ID externe. L'ID externe peut être n'importe quel mot ou nombre convenu avec l'administrateur du compte tiers. Cette option ajoute automatiquement une condition à la politique de confiance qui permet à l'utilisateur d'assumer le rôle uniquement si la demande inclut le STS:ExternalId correct. Pour plus d'informations, consultez Comment utiliser un identifiant externe lorsque vous accordez l'accès à vos AWS ressources à un tiers.
   - Si vous souhaitez limiter le rôle aux utilisateurs qui se connectent à l'aide de l'authentification multifactorielle (MFA), choisissez Exiger MFA. Cela ajoute une condition à la politique d'approbation du rôle qui exige une authentification MFA. Un utilisateur qui veut endosser le rôle doit se connecter avec un mot de passe unique temporaire à partir d'un dispositif MFA configuré. Les utilisateurs ne disposant pas d'une authentification MFA ne peuvent pas assumer ce rôle. Pour plus d'informations sur l'authentification multifactorielle, consultez la section Utilisation de l'authentification multifactorielle (MFA) dans. AWS
5. Choisissez Suivant : Autorisations.

   IAM inclut une liste de politiques dans le compte. Sous Ajouter des autorisations, saisissez amspatchmanagedpolicy dans la zone de filtre et cochez la case correspondant à cette politique d'autorisations. Cliquez sur Next (Suivant).
6. Sous Détails du rôle, entrez un nom de rôle tel que PatchRole, ajoutez une description du rôle (recommandé), ajoutez également des balises pour vous aider à identifier ce rôle. Les noms de rôles ne distinguent pas les majuscules des minuscules, mais doivent être uniques dans le Compte AWS. Lorsque vous avez terminé, cliquez sur Créer un rôle.

   > **Note**
   >
   > Les noms de rôles ne peuvent pas être modifiés une fois qu'ils ont été créés.

Comprendre les notifications relatives aux correctifs et les défaillances des correctifs dans AMS Accelerate

Important

À compter du 1er février 2025, les clients AMS ne recevront plus de notifications pour les fenêtres de maintenance des correctifs vides dans leurs comptes gérés.

Demandes de service de correctifs et notifications par e-mail

AMS crée une nouvelle demande de service quatre jours avant la prochaine fenêtre de maintenance des correctifs. Par exemple, quatre jours avant l'exécution d'une fenêtre de maintenance des correctifs nommée App1 PROD, AMS crée une demande de service intitulée Fenêtre de maintenance des correctifs d'avril pour App1 Prod for Account [identifiant de compte]. Utilisez la demande de service de correctifs pour communiquer avec AMS si vous avez besoin d'apporter des modifications à votre correctif planifié ou pour ignorer un correctif à venir. Lorsqu'une demande de service est créée, un e-mail est envoyé à votre adresse de notification de correctif avec un lien vers la demande de service. Vous recevez un e-mail supplémentaire chaque fois qu'AMS met à jour la demande de service.

Note

AMS crée une nouvelle demande de service, même si la fenêtre de maintenance des correctifs est créée moins de quatre jours avant la date prévue pour son exécution. La fenêtre de maintenance des correctifs doit être « activée » pour recevoir des notifications de demande de service.

Une heure avant le début de l'application des correctifs, AMS vous en informe par le biais de la demande de service de correctifs. Une fois l'application des correctifs terminée, AMS met à jour la demande de service de correctifs avec un lien vers la console Patch Manager. Utilisez le lien pour voir la conformité des correctifs pour les instances ciblées par la fenêtre de maintenance des correctifs.

> **Note**
>
> Les liens de la console Patch Manager indiquent la conformité actuelle des instances. Le gestionnaire de correctifs indique qu'une instance n'est pas conforme si de nouveaux correctifs sont publiés entre le moment où AMS termine l'application des correctifs et celui où vous accédez au lien.

Notifications de correctifs via CloudWatch des événements

AMS envoie CloudWatch des événements à trois reprises au cours du processus de correction, notamment les suivants :

- Quatre jours avant l'ouverture de la fenêtre de maintenance des correctifs.
- Une heure avant l'ouverture de la fenêtre de maintenance des correctifs.
- Lorsque la fenêtre de maintenance des correctifs est terminée.

Voici le schéma des événements de notification avancée de la fenêtre de maintenance des correctifs :

```
{
    "version": "0",
    "id": "37004d81-458d-2cef-fe1c-8afa8af30406",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "145917996532",
    "time": "2021-05-20T02:00:00Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {
        "State": "PREEMPTIVE",
        "StartTime": "2021-05-24T02:00:00.000000",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\"}, {\"instanceId\":
 \"i-0000000aaaaaaaaab\"}]"
```

```
    }
}
```

Le tableau suivant décrit le schéma des événements de notification préalable de la fenêtre de maintenance des correctifs :

Détails des notifications relatives aux correctifs

Nom de la propriété	Description	Exemples de valeurs
État	État de la fenêtre de maintenance des correctifs	PREEMPTIVE - La fenêtre d'application des correctifs devrait bientôt commencer
Status	État de la fenêtre de maintenance des correctifs	SUCCÈS - Toutes les instances ont été corrigées sans échec ÉCHEC : le correctif d'au moins une instance n'a pas pu être corrigé
StartTime	Heure de début, au format ISO, de la fenêtre de maintenance des correctifs	03/02/2021 22:14:05 .814 308
WindowArn	Identifiant unique de la fenêtre de maintenance des correctifs	arn:aws:ssm:us-east-1 : 123456789012 : fenêtre de maintenance/mw-000 00001235
Résultats	La liste des instances ciblées par la fenêtre de correctifs	InstanceId — l'ID d'instance de l'instance ciblée

Voici le schéma des événements de fin de fenêtre de maintenance des correctifs :

```
{"version": "0",
    "id": "0f25add5-44a9-0702-d2bc-bd2102affefe",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
```

```
    "account": "123456789012",
    "time": "2021-02-03T22:14:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {"State": "[COMPLETED]",
        "Status": "SUCCESS",
        "StartTime": "2021-02-03T22:12:00.814308",
        "EndTime": "2021-02-03T22:14:05.814309",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "WindowExecutionId": "e32088eb-c05f-4c63-b766-6866e163c818",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\", \"status\":
 \"Success\", \"missing_critical_patch_count\": 0, \"missing_total_patch_count
\": 0} }, {\"instanceId\": \"i-0000000aaaaaaaaab\", \"status\": Success},
 \"missing_critical_patch_count\": 0, \"missing_total_patch_count\": 0}]"
    }
}
```

Le tableau suivant décrit le schéma des événements de fin de fenêtre de maintenance des correctifs :

Détails de fin de fenêtre de patch

Nom de la propriété	Description	Exemples de valeurs
État	État de la fenêtre de maintenance des correctifs	TERMINÉ — La fenêtre d'application des correctifs est terminée
Status	État de la fenêtre de maintenance des correctifs	SUCCÈS — Toutes les instances ont été corrigées sans échec ÉCHEC : le correctif d'au moins une instance n'a pas pu être corrigé

Nom de la propriété	Description	Exemples de valeurs
StartTime	Heure de début, au format ISO, de la fenêtre de maintenance des correctifs	03/02/2021 22:14:05 .814 308
EndTime	Heure de fin, au format ISO, de la fenêtre de maintenance des correctifs	03/02/2021 23:14:05 .814 308
WindowArn	Identifiant unique de la fenêtre de maintenance des correctifs.	arn:aws:ssm:us-east-1 : 123456789012 : fenêtre de maintenance/mw-000 00001235
WindowExecutionId	L'ID d'exécution de la fenêtre, visible depuis la console de fenêtre de maintenance SSM	e32088eb-c05f-4c63-b766-6866e163c818
Résultats	La liste des instances qui seront ciblées par la fenêtre de correctif	InstanceId — l'ID d'instance ciblé status : état du correctif de l'instance missing_critical_patch_coun t : le nombre de correctif s critiques manquants sur l'instance missing_total_patch_count : le nombre total de correctifs manquants sur l'instance

Vous pouvez utiliser l'événement CloudWatch Events pour déclencher une CloudWatch règle qui vous avertit lorsqu'un préavis relatif à la fenêtre de maintenance des correctifs est envoyé. Pour ce faire, configurez la CloudWatch règle avec la configuration suivante :

```
{
    "source": [
        "aws.managedservices"
    ],
    "detail-type": [
        "AMS Patch Window Execution State Change"
    ],
    "detail": {
        "State": ["PREEMPTIVE"]
    }
}
```

> **Note**
>
> Les alertes d'échec des correctifs ne sont pas créées pour les instances dont les systèmes d'exploitation ne sont pas pris en charge ou qui sont arrêtées pendant la période de maintenance.

Enquête sur les défaillances des correctifs dans AMS

AWS Managed Services (AMS) gère les correctifs et inclut la correction des défaillances des correctifs. Lorsque le correctif échoue, AMS Operations est alerté et tente de remédier au problème en suivant les meilleures pratiques AWS d'AMS pour résoudre le problème.

<instance-id>Si un correctif échoue, AMS crée un SSM OpsItem dans le compte avec le titre suivant : AWS Managed Services — Patch Instance failure, par exemple.

AMS enquête ensuite sur le. OpsItem Si AMS peut corriger la panne sans votre intervention, AMS résout le problème OpsItem. Si votre intervention est requise, AMS vous en informe par le biais d'une demande de service contenant les résultats de l'enquête et les mesures correctives recommandées. Si vous ne prenez aucune mesure pour résoudre le problème, AMS tente de corriger l'instance lors de la prochaine fenêtre de maintenance des correctifs planifiée.

> **Note**
>
> OpsItems Les défaillances des correctifs ne sont pas créées pour les instances dont les systèmes d'exploitation ne sont pas pris en charge ou dont l'état est arrêté pendant la fenêtre de maintenance des correctifs.

Optimisation des coûts avec AMS Resource Scheduler

La AWS solution AMS Resource Scheduler vous aide à réduire vos coûts AWS et ceux d'AMS en arrêtant les ressources qui ne sont pas utilisées et en démarrant les ressources lorsque de la capacité est nécessaire. Par exemple, vous pouvez utiliser AMS Resource Scheduler AWS dans un environnement de développement pour arrêter automatiquement les instances en dehors des heures de bureau tous les jours. Si vous laissez toutes vos instances fonctionner à pleine capacité, cette solution peut entraîner une réduction du taux d'utilisation des instances, ce qui réduit le coût global en fonction des plannings que vous configurez.

Utilisez le planificateur de ressources AWS Managed Services (AMS) pour planifier le démarrage et l'arrêt automatiques des groupes Auto Scaling, des EC2 instances Amazon et des instances Amazon RDS dans votre compte. Cela permet de réduire les coûts d'infrastructure lorsque les ressources ne sont pas censées fonctionner 24 heures sur 24, 7 jours sur 7. La solution repose sur AWS Instance Scheduler mais contient des fonctionnalités supplémentaires et des personnalisations spécifiques aux besoins des clients AMS. La personnalisation inclut la prise en charge de la planification des groupes Auto Scaling, un suppresseur CloudWatch d'alarme pour les alarmes Elastic Load Balancing, la prise en charge de plusieurs fenêtres de AWS Systems Manager maintenance pour Amazon EC2, un estimateur d'économies de coûts et le support opérationnel d'AMS.

AMS Resource Scheduler utilise des périodes et des plannings. Les périodes définissent les heures pendant lesquelles la ressource doit s'exécuter, telles que l'heure de début, l'heure de fin et les jours du mois. Les plannings contiennent les périodes que vous avez définies, ainsi que des configurations supplémentaires (fenêtre de maintenance SSM, fuseau horaire, hibernation, etc.) et spécifient le moment où les ressources doivent être exécutées. Vous pouvez configurer ces périodes et ces horaires à l'aide des runbooks d' AWS Systems Manager automatisation fournis par AMS. Chaque calendrier doit contenir au moins une période qui définit la ou les heures auxquelles l'instance doit s'exécuter. Un calendrier peut contenir plusieurs périodes. Lorsque plusieurs périodes sont utilisées dans un calendrier, le planificateur d'instances applique l'action de démarrage appropriée lorsqu'au moins une des règles relatives aux périodes est vraie. Pour plus de détails sur le calendrier et les périodes, consultez Solutions Components of AWS Instance Scheduler.

Le planificateur de ressources AMS utilise AWS des balises de ressources pour associer un calendrier à une ou plusieurs ressources afin de les cibler pour des actions de démarrage et d'arrêt planifiées. Vous balisez vos ressources à l'aide de la clé de balise (par défaut`Schedule`) configurée dans le planificateur avec le nom du calendrier comme valeur. Vous configurez la même clé de balise

que la balise de répartition des coûts AWS Cost Explorer pour la fonction d'estimateur de coûts du planificateur afin de suivre et de signaler les économies de coûts.

Le planificateur de ressources AMS est une fonctionnalité facultative que vous pouvez activer par compte.

Utilisation des ressources avec AMS Resource Scheduler

Amazon EC2

- Les EC2 instances Amazon qui font partie d'un groupe Auto Scaling ne sont pas traitées individuellement et ne sont pas prises en compte par AMS Resource Scheduler, même si elles sont étiquetées.
- Si le volume racine de l'instance cible est chiffré à l'aide d'une clé principale AWS KMS client (CMK), une `kms:CreateGrant` autorisation supplémentaire doit être ajoutée à votre rôle IAM de planificateur de ressources pour que le planificateur puisse démarrer de telles instances. Cette autorisation n'est pas ajoutée au rôle par défaut pour améliorer la sécurité. Si vous avez besoin de cette autorisation, vous pouvez l'ajouter en mettant à jour la CloudFormation pile`ams-resource-scheduler`, avec une liste de CMK comme valeur du `UseCMK` paramètre (utilisez une ou plusieurs clés CMK `arn:`*`partition`*`:kms:`*`region`*`:`*`account-id`*`:key/`*`key-id`* au format ARNs au lieu d'un alias KMS).
- Si vos EC2 instances Amazon sont configurées avec un logiciel spécifique ou des licences fournisseurs gérées par AWS License Manager, Resource Scheduler a besoin des autorisations relatives aux AWS License Manager licences spécifiques pour pouvoir démarrer l'instance. Vous pouvez accorder à Resource Scheduler les autorisations nécessaires en ajoutant la liste des ARN des AWS License Manager licences au paramètre de licence EC2 par exemple du gestionnaire de licences de la CloudFormation pile ()`ams-resource-scheduler`.

Amazon EC2 Auto Scaling

- AMS Resource Scheduler démarre ou arrête le dimensionnement automatique des groupes Auto Scaling, et non des instances individuelles du groupe. C'est-à-dire que le planificateur rétablit la taille du groupe Auto Scaling (start) ou définit la taille sur 0 (stop).
- Marquez le groupe Auto Scaling avec le tag spécifié et non les instances du groupe.
- Pendant l'arrêt, AMS Resource Scheduler enregistre les valeurs de capacité minimale, souhaitée et maximale du groupe Auto Scaling et définit les capacités minimale et souhaitée sur 0. Au

démarrage, le planificateur rétablit la taille du groupe Auto Scaling telle qu'elle était lors de l'arrêt. Par conséquent, les instances du groupe Auto Scaling doivent utiliser une configuration de capacité appropriée afin que la fermeture et le redémarrage des instances n'affectent aucune application exécutée dans le groupe Auto Scaling.

- Si le groupe Auto Scaling est modifié (capacité minimale ou maximale) pendant une période d'exécution, le planificateur enregistre la nouvelle taille du groupe Auto Scaling et l'utilise lors de la restauration du groupe à la fin d'un calendrier d'arrêt.

Amazon RDS

- Le planificateur peut prendre un instantané avant d'arrêter les instances RDS (cela ne s'applique pas au cluster de base de données Aurora). Cette fonctionnalité est activée par défaut lorsque le paramètre du CloudFormation modèle AWS Create RDS Instance Snapshot est défini sur true. L'instantané est conservé jusqu'au prochain arrêt de l'instance Amazon RDS et à la création d'un nouvel instantané.
- Le planificateur peut utiliser des instances start/stop Amazon RDS faisant partie d'un cluster ou d'une base de données Amazon RDS Aurora ou dans une configuration de zones de disponibilité multiples (multi-AZ). Vérifiez toutefois les limites d'Amazon RDS lorsque le planificateur ne sera pas en mesure d'arrêter l'instance Amazon RDS, en particulier les instances multi-AZ.
- Pour planifier le démarrage ou l'arrêt d'Aurora Cluster, utilisez le paramètre de modèle Schedule Aurora Clusters (la valeur par défaut est true). Le cluster Aurora (et non les instances individuelles du cluster) doit être étiqueté avec la clé de balise définie lors de la configuration initiale et le nom du planning comme valeur de balise pour planifier ce cluster.

> **Note**
>
> Le planificateur de ressources ne valide pas le démarrage ou l'arrêt d'une ressource. Il fait appel à l'API pour le service concerné et passe à autre chose. Si l'appel d'API échoue, il enregistre l'erreur à des fins d'investigation.
> Le planificateur de ressources AMS ne prend pas en charge AWS Backup les fenêtres.
> Si vous mappez une instance RDS AWS Backup activée avec le planning du Resource Scheduler, pour que la sauvegarde fonctionne comme prévu, la fenêtre de sauvegarde doit se trouver dans la fenêtre d'exécution du planning.

Intégration du planificateur de ressources AMS

Votre compte n'est pas automatiquement intégré à AMS Resource Scheduler lorsqu'il est intégré au plan d'opérations AMS Accelerate. Toutefois, dans le cadre de l'intégration du compte au plan d'exploitation AMS Accelerate, ou à tout moment par la suite, vous pouvez demander à votre responsable de prestation de services cloud (CSDM) d'intégrer le compte à AMS Resource Scheduler. Une fois que votre CSDM a intégré le compte, une CloudFormation pile contenant des ressources AMS Resource Scheduler avec une configuration par défaut est automatiquement provisionnée dans votre compte.

Une fois le planificateur de ressources AMS configuré dans votre compte, nous vous recommandons de revoir la configuration par défaut et, si nécessaire, de personnaliser les configurations telles que la clé de balise, le fuseau horaire, les services planifiés, etc., en fonction de vos préférences. Pour plus de détails sur les personnalisations recommandéesPersonnalisation du planificateur de ressources AMS, reportez-vous à la section suivante.

Personnalisation du planificateur de ressources AMS

Une fois intégré, le planificateur de ressources AMS est déployé sous forme de CloudFormation pile, avec un nom`ams-resource-scheduler`, dans la région AWS principale de votre compte AMS Accelerate. Vous pouvez configurer les propriétés d'AMS Resource Scheduler en fonction de vos préférences via les paramètres de CloudFormation pile et en effectuant une mise à jour de la pile. Pour plus d'informations sur la mise à jour CloudFormation des piles, consultez la section Mise à jour directe des piles.

Nous vous recommandons de personnaliser les propriétés suivantes et de laisser le reste par défaut pour une fonctionnalité optimale.

- Nom de balise : nom de la balise que le planificateur de ressources utilisera pour associer les plannings d'instance aux ressources. La valeur par défaut est `Schedule`.
- Service (s) à planifier : liste séparée par des virgules des services que le planificateur de ressources peut gérer. La valeur par défaut est « `ec2,rds,autoscaling` ». Les valeurs valides sont « ec2 », « rds » et « autoscaling ».
- Fuseau horaire par défaut : Spécifiez le fuseau horaire par défaut que le planificateur de ressources doit utiliser. La valeur par défaut est `UTC`.

- CMK pour les volumes EBS chiffrés : liste séparée par des virgules des clés gérées par le client (CMK) Amazon KMS pour lesquelles le Resource Scheduler peut être ARNs autorisé à obtenir des autorisations.
- Licence de gestionnaire de licences, EC2 par exemple : une liste séparée par des virgules d'AWS License Manager ARNs pour laquelle le Resource Scheduler peut être autorisé.

> **Note**
>
> AMS publie occasionnellement des fonctionnalités et des correctifs pour maintenir le planificateur de ressources AMS à jour sur votre compte. Dans ce cas, toute personnalisation que vous apportez à la pile AMS Resource Scheduler via les paramètres de la pile est préservée.
> Nous vous recommandons vivement de ne pas personnaliser directement l'une des ressources des composants d'AMS Resource Scheduler. Cela a un impact sur les fonctionnalités du planificateur de ressources et sur la capacité d'AMS à le maintenir à jour.

Utilisation du planificateur de ressources AMS

Comment utiliser les périodes du planificateur de ressources AMS dans les comptes AMS Accelerate.

Utilisez l'ensemble de runbooks d' AWS Systems Manager automatisation suivant pour administrer le calendrier et la période requis dans AMS Resource Scheduler.

> **Note**
>
> Ces runbooks d'automatisation SSM sont disponibles dans la région AWS principale de votre compte.

- `AWSManagedServices-AddOrUpdatePeriod`
- `AWSManagedServices-AddOrUpdateSchedule`
- `AWSManagedServices-DeleteScheduleOrPeriod`
- `AWSManagedServices-DescribeScheduleOrPeriods`
- `AWSManagedServices-EnableOrDisableAMSResourceScheduler`

En outre, AMS AWS Identity and Access Management fournit un rôle qui AWS Systems Manager nécessite et assume pour utiliser les runbooks. `ams_resource_scheduler_ssm_automation_role` Le rôle IAM est limité par une politique en ligne du moindre privilège octroyant les autorisations SSM requises pour le fonctionnement des runbooks.

Prérequis

Effectuez les étapes suivantes avant de commencer à utiliser le runbook d'automatisation SSM et le planificateur de ressources AMS.

Attachez la politique suivante à l'entité IAM appropriée (utilisateur, groupe ou rôle) que vous souhaitez autoriser à utiliser les runbooks d'automatisation pour administrer le calendrier et la période dans le planificateur de ressources AMS. La politique n'est pas requise si votre entité IAM dispose d'une autorisation d'administrateur ou d'une PowerUser autorisation sur votre compte.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPassingResourceSchedulerRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/
ams_resource_scheduler_ssm_automation_role",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Sid": "ListAndDescribeAutomationExecutions",
            "Effect": "Allow",
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:DescribeAutomationStepExecutions"
            ],
            "Resource": "arn:aws:ssm:*:111122223333:automation-execution/*"
        },
```

```
        {
            "Sid": "ListAndDescribeResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:ListDocumentVersions",
                "ssm:DescribeDocument",
                "ssm:ListDocumentMetadataHistory",
                "ssm:DescribeDocumentParameters",
                "ssm:GetDocument",
                "ssm:DescribeDocumentPermission"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdatePeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdateSchedule",
                "arn:aws:ssm:*::document/AWSManagedServices-
DeleteScheduleOrPeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-
DescribeScheduleOrPeriods",
                "arn:aws:ssm:*::document/AWSManagedServices-
EnableOrDisableAMSResourceScheduler"
            ]
        },
        {
            "Sid": "AllowExecutionOfResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
AddOrUpdatePeriod:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
AddOrUpdateSchedule:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
DeleteScheduleOrPeriod:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
DescribeScheduleOrPeriods:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
EnableOrDisableAMSResourceScheduler:*"
            ]
        },
        {
            "Sid": "AllowListingAllDocuments",
            "Effect": "Allow",
```

```
            "Action": "ssm:ListDocuments",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingAllSSMExecutions",
            "Effect": "Allow",
            "Action": "ssm:DescribeAutomationExecutions",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingIAMRolesForStartingExecutionViaConsole",
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        }
    ]
}
```

Vous pouvez exécuter l'automatisation à partir de la AWS Systems Manager console ou à l'aide de la AWS CLI. Si vous utilisez la AWS CLI, vous devrez peut-être l'installer et la configurer ou les AWS outils nécessaires PowerShell, si ce n'est déjà fait. Pour plus d'informations, voir Installer ou mettre à niveau les outils de ligne de AWS commande.

Regardez la vidéo de Navish pour en savoir plus (4:52)

Utilisation des périodes et des plannings dans AWS Managed Services Resource Scheduler

Vous pouvez utiliser le planificateur de ressources AMS pour ajouter, mettre à jour ou supprimer des plannings ou des périodes dans les comptes AMS Accelerate.

Ajouter ou mettre à jour des périodes dans le planificateur de ressources AMS

Ajoutez ou mettez à jour une période du planificateur de ressources dans vos comptes AMS.

Les données dont vous aurez besoin :

- Action : type d'opération à effectuer. Utilisez « ajouter » si vous souhaitez ajouter une période ou « mettre à jour » si vous souhaitez mettre à jour une période existante.
- Nom : nom de la période. Vous devez spécifier une valeur unique si vous ajoutez une nouvelle période.

- AutomationAssumeRole: ARN du rôle AWS Identity and Access Management (IAM) qui permet au runbook d'ajouter ou de mettre à jour la période en votre nom. Spécifiez le rôle en tant que`ams_resource_scheduler_ssm_automation_role`.
- Description (facultatif) : description significative de la période.
- BeginTime(Facultatif) : Heure au format HH:MM à laquelle vous souhaitez démarrer les ressources.
- EndTime(Facultatif) : Heure au format HH:MM à laquelle vous souhaitez arrêter les ressources.
- Mois (facultatif) : liste de mois séparés par des virgules ou intervalle de mois avec un trait d'union pendant lesquels les ressources doivent être exécutées.
- MonthDays(Facultatif) : liste des jours du mois séparés par des virgules ou intervalle de jours pendant lesquels les ressources doivent être exécutées avec un trait d'union.
- WeekDays(Facultatif) : liste séparée par des virgules des jours de la semaine ou d'une plage de jours de la semaine pendant lesquels les ressources doivent être exécutées.

Comment le faire :

- Consultez le document à l' AWSManagedServices-AddOrUpdatePeriodadresse (vous devrez peut-être choisir votre région d'intégration).

  Spécifiez les exigences dans la section Paramètres d'entrée, puis choisissez Execute. Une fois l'opération terminée, consultez les résultats dans l'onglet Sortie.
- AWS CLI :

  Exécutez la commande suivante pour démarrer une automatisation. Remplacez *placeholders* par vos propres informations.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdatePeriod" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"],
    "Description":["DESCRIPTION"],"BeginTime":["TIME"], "EndTime":["TIME"],
    "Months":["MONTH"],"MonthDays":["DAY"], "WeekDays":["DAY"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

Exemple :

L'exemple suivant montre comment ajouter une nouvelle période à l'aide de la AWS Systems Manager console. Nous avons nommé la période Period-Name et l'avons configurée pour couvrir la période de 9 h à 18 h du lundi au vendredi pendant les 15 premiers jours de chaque mois.

1. Consultez le document AWS Systems Manager d'automatisation à l'adresse AWSManagedServices-AddOrUpdatePeriod(vous devrez peut-être choisir votre région intégrée).

2. Fournissez des valeurs pour les paramètres.

3. Cliquez sur Exécuter et attendez que l'automatisation soit terminée.

Ajouter ou mettre à jour des plannings dans le planificateur de ressources AMS

Ajoutez ou mettez à jour un calendrier de planificateur de ressources dans les comptes AMS Accelerate.

Les données dont vous aurez besoin :

- Action : type d'opération à effectuer. Utilisez « ajouter » si vous souhaitez ajouter un calendrier ou « mettre à jour » si vous souhaitez mettre à jour un calendrier existant.
- Nom : nom du planning. Vous devez spécifier une valeur unique si vous ajoutez un nouveau calendrier.
- AutomationAssumeRole: ARN du rôle AWS Identity and Access Management (IAM) qui permet au runbook d'ajouter ou de mettre à jour le calendrier en votre nom. Spécifiez le rôle`ams_resource_scheduler_ssm_automation_role`.
- Description (facultatif) : description significative du calendrier.
- Horaires (facultatif) : Spécifiez une liste de périodes séparées par des virgules à utiliser avec ce calendrier. Chaque période doit déjà avoir été créée.
- RetainRunning(Facultatif) : Spécifiez « vrai » pour empêcher le planificateur de ressources d'arrêter une ressource en cours d'exécution à la fin d'une période d'exécution si la ressource a été démarrée manuellement avant le début de la période d'exécution. Par défaut, le planificateur de ressources arrête la ressource.
- StopNewInstances(Facultatif) : Spécifiez « false » pour empêcher le planificateur de ressources d'arrêter une ressource la première fois qu'elle est étiquetée si elle est exécutée en dehors de la période d'exécution. Par défaut, le planificateur de ressources arrête la ressource.

- SSMMaintenanceFenêtre (facultatif) : Spécifiez une liste séparée par des virgules des fenêtres de maintenance AWS Systems Manager (SSM) que vous souhaitez ajouter en tant que périodes de fonctionnement pour le calendrier. Vous devez également attribuer à la propriété UseMaintenanceWindow « » la valeur « true ».
- TimeZone(Facultatif) : Spécifiez le fuseau horaire que le planificateur de ressources doit utiliser. Par défaut, le planificateur de ressources utilise l'UTC.
- UseMaintenanceWindow(Facultatif) : Spécifiez « true » si vous souhaitez que le Resource Scheduler considère la fenêtre de maintenance d'Amazon Relational Database Service (RDS) comme une période d'exécution d'un calendrier d'instance Amazon RDS, ou pour ajouter les fenêtres de maintenance d'AWS Systems Manager (SSM) comme période d'exécution à un calendrier d'instance Amazon. EC2
- UseMetrics(Facultatif) : Spécifiez « vrai » pour activer CloudWatch les métriques au niveau de la planification et « faux » pour désactiver CloudWatch les métriques. La spécification de cette propriété remplace le paramètre de CloudWatch métriques défini au niveau de la pile.

Comment le faire :

- Consultez le document à l' AWSManagedServices-AddOrUpdateScheduleadresse (vous devrez peut-être choisir votre région d'intégration).

  Spécifiez les exigences dans la section Paramètres d'entrée, puis choisissez Execute. Une fois l'opération terminée, consultez les résultats dans l'onglet Sortie.
- AWS CLI :

  Exécutez la commande suivante pour démarrer une automatisation. Remplacez *placeholders* par vos propres informations.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdateSchedule" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"], "Description":
["DESCRIPTION"],
    "Hibernate":["true or false"],"Enforced":["true or false"],
    "OverrideStatus":["running or stopped"],"Periods":["PERIOD-A, PERIOD-B"],
    "RetainRunning":["true or false"],"StopNewInstances":["true or false"],
    "SSMMaintenanceWindow":["WINDOW-NAME"],"TimeZone":["TIMEZONE"],
    "UseMaintenanceWindow":["true or false"],"UseMetrics":["true or false"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

Exemple :

L'exemple suivant montre comment ajouter un calendrier pour AMS Resource Scheduler. Dans cet exemple, vous ajoutez un calendrier nommé CustomSchedule using CustomPeriod.

1. Consultez le document AWS Systems Manager d'automatisation à l'adresse AWSManagedServices-AddOrUpdateSchedule(vous devrez peut-être choisir votre région intégrée).

2. Fournissez des valeurs pour les paramètres.

3. Cliquez sur Exécuter et attendez que l'automatisation soit terminée.

Supprimer des périodes ou des plannings dans le planificateur de ressources AMS

Pour supprimer les périodes ou les plannings du Resource Scheduler dans les comptes AMS Accelerate, vous avez besoin des données suivantes :

- ConfigurationType: le type de configuration que vous souhaitez supprimer. Utilisez « période » pour supprimer des périodes ou « calendrier » pour supprimer des plannings.
- Nom : nom du calendrier ou de la période que vous souhaitez supprimer.
- AutomationAssumeRole: ARN du rôle AWS Identity and Access Management (IAM) qui permet au runbook de supprimer des plannings ou des périodes en votre nom. Spécifiez le rôle`ams_resource_scheduler_ssm_automation_role`.

Comment le faire :

- Consultez le document à l'adresse AWSManagedServices-DeleteScheduleOrPeriod(il se peut que vous deviez choisir votre région intégrée).

  Spécifiez les exigences dans la section Paramètres d'entrée, puis choisissez Execute. Une fois l'opération terminée, consultez les résultats dans l'onglet Sortie.

- AWS CLI :

  Exécutez la commande suivante pour démarrer une automatisation. Remplacez *`placeholders`* par vos propres informations.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DeleteScheduleOrPeriod" --document-version "\$DEFAULT"
--parameters '{"ConfigurationType":["period" or "schedule"],"Name":["NAME"],
    "AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}' --region ONBOARDED_REGION
```

Exemple :

L'exemple suivant montre comment supprimer un point à l'aide de la AWS Systems Manager console.

1. Consultez le document AWS Systems Manager d'automatisation à l'adresse AWSManagedServices-DeleteScheduleOrPeriod(vous devrez peut-être choisir votre région intégrée).

2. Fournissez des valeurs pour les paramètres.

3. Cliquez sur Exécuter et attendez que l'automatisation soit terminée.

Décrire les périodes ou les plannings dans le planificateur de ressources AMS

Pour décrire (afficher des détails sur) une période ou un calendrier du planificateur de ressources dans les comptes AMS Accelerate, vous avez besoin des données suivantes :

- ConfigurationType: le type de configuration que vous souhaitez décrire. Utilisez « périodes » pour décrire toutes les périodes ou « calendriers » pour décrire tous les programmes.
- AutomationAssumeRole: l'ARN du rôle AWS Identity and Access Management (IAM) qui permet au runbook de décrire les plannings ou les périodes en votre nom. Spécifiez le rôle`ams_resource_scheduler_ssm_automation_role`.

Comment le faire :

- Consultez le document à l' AWSManagedServices-DescribeScheduleOrPeriodsadresse (vous devrez peut-être choisir votre région d'intégration) :
  1. Spécifiez les exigences dans la section Paramètres d'entrée, puis choisissez Execute.
  2. Une fois l'opération terminée, consultez les résultats dans l'onglet Sortie.

- AWS CLI :
  1. Exécutez la commande suivante pour démarrer une automatisation. Remplacez *placeholders* par vos propres informations.

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DescribeScheduleOrPeriods" --document-version "\$DEFAULT"
                --parameters '{"ConfigurationType":["period" or
 "schedule"],"AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}'
                --region ONBOARDED_REGION
```

Exemple :

L'exemple suivant montre comment décrire une période à l'aide de la AWS Systems Manager console.

1. Consultez le document AWS Systems Manager d'automatisation à l'adresse AWSManagedServices-DescribeScheduleOrPeriods(vous devrez peut-être choisir votre région intégrée).

2. Fournissez des valeurs pour les paramètres.

3. Cliquez sur Exécuter et attendez que l'automatisation soit terminée.

Ressources de balisage pour AMS Resource Scheduler

Ressources de balisage pour AMS Resource Scheduler.

Une fois que vous avez ajouté des horaires et des périodes à AMS Resource Schedule, vous devez étiqueter vos ressources avec le nom de balise Resource Scheduler comme clé de balise, ou le nom du calendrier comme clé de balise, et le nom du calendrier comme valeur de balise. Pour plus de détails sur la façon de baliser vos ressources dans votre compte AMS Accelerate, consultezMarquage dans AMS Accelerate.

> **Note**
>
> Si le Resource Tagger est utilisé pour étiqueter les ressources, la clé de balise par défaut du Resource Scheduler doit être personnalisée pour avoir le préfixe « `ams:rt:` », car toutes

les balises appliquées par le baliseur de ressources ont le préfixe de clé « ». `ams:rt:` Dans le cas contraire, les ressources étiquetées avec le marqueur de ressources ne seront pas gérées par le Resource Scheduler. Pour en savoir plus sur la personnalisation de la clé de balise par défaut pour le planificateur de ressources, consultez. Personnalisation du planificateur de ressources AMS

Estimateur de coûts dans AMS Resource Scheduler

Afin de suivre les économies de coûts, AMS Resource Scheduler comporte un composant qui calcule toutes les heures les économies estimées pour les ressources Amazon et EC2 Amazon RDS gérées par le planificateur. Ces données de réduction des coûts sont ensuite publiées sous forme de CloudWatch métrique (`AMS/ResourceScheduler`) pour vous aider à les suivre. L'estimateur d'économies de coûts estime uniquement les économies réalisées sur les heures de fonctionnement des instances. Il ne prend pas en compte les autres coûts, tels que les coûts de transfert de données associés à une ressource.

L'estimateur d'économies de coûts est activé avec le planificateur de ressources. Il fonctionne toutes les heures et extrait les données sur les coûts et l'utilisation à partir de AWS Cost Explorer. À partir de ces données, il calcule le coût horaire moyen pour chaque type d'instance, puis projette le coût pour une journée complète si l'instance était exécutée sans être planifiée. Les économies de coûts correspondent à la différence entre le coût prévu et le coût réel indiqué par Cost Explorer pour un jour donné.

Par exemple, si l'instance A est configurée avec le planificateur de ressources pour fonctionner de 9 h à 17 h, cela représente huit heures par jour. Cost Explorer indique que le coût est de 1$ et que l'utilisation est de 8$. Le coût horaire moyen est donc de 0,125$. Si l'instance n'était pas planifiée avec le planificateur de ressources, elle s'exécuterait 24 heures sur 24 ce jour-là. Dans ce cas, le coût aurait été de 24 x 0,125 = 3$. Le planificateur de ressources vous a permis de réaliser des économies de 2$.

Pour que l'estimateur d'économies puisse récupérer les coûts et l'utilisation uniquement pour les ressources gérées par Resource Scheduler à partir de Cost Explorer, la clé de balise que le planificateur de ressources utilise pour cibler les ressources doit être activée en tant que balise de répartition des coûts dans le tableau de bord de facturation. Si le compte appartient à une organisation, la clé du tag doit être activée dans le compte de gestion de l'organisation. Pour plus d'informations sur cette procédure, voir Activation des balises de répartition des coûts définies par l'utilisateur et des balises de répartition des coûts définies par l'utilisateur

Une fois que la clé de balise est activée en tant que balise de répartition des coûts, AWS Billing commence à suivre les coûts et l'utilisation des ressources gérées par Resource Scheduler, et une fois ces données disponibles, l'estimateur d'économies de coûts commence à calculer les économies de coûts et à publier les données sous l'`AMS/ResourceScheduler`espace de noms métrique dans. CloudWatch

Si l'étiquette de répartition des coûts n'est pas activée, l'estimateur n'est pas en mesure de calculer les économies et de publier la métrique, même si elle est activée.

> **Note**
>
> Cost Savings Estimator n'accepte pas les remises telles que les instances réservées, les plans d'épargne, etc., dans son calcul. L'estimateur prend les coûts d'utilisation de Cost Explorer et calcule le coût horaire moyen des ressources. Pour plus de détails, voir Comprendre vos ensembles de données de AWS coûts : un aide-mémoire.

Suppresseur d'alarme dans le planificateur de ressources AMS

AMS Resource Scheduler est fourni avec un suppresseur CloudWatch d'alarme, déployé sous la forme d'une fonction Lambda distincte nommée `AMSAlarmSuppressor` qui supprime les alarmes pour les instances situées derrière un Elastic Load Balancing, un Application Load Balancer ou un Network Load Balancer. La fonction s'exécute toutes les 5 minutes, récupère toutes les alarmes présentes dans le compte et les regroupe en fonction de l'espace de noms ; par exemple,`AWS/ELB`,`AWS/ApplicationELB`. `AWS/NetworkELB` Pour chaque groupe d'alarmes, le suppresseur trouve le nom de l'équilibreur de charge, le groupe and/or cible (pour le groupe ALB/NLB) from alarm dimensions, finds the instances that are registered with the load balancer and/or cible) et vérifie l'état de l'instance pour découvrir si les instances sont planifiées par AMS Resource Scheduler. Si les instances sont planifiées par le planificateur de ressources et sont arrêtées par le planificateur de ressources, le suppresseur marque ensuite les alarmes pour les désactiver. Si au moins une instance de la liste des instances enregistrées est en cours d'exécution, le suppresseur marque les alarmes correspondantes pour activer les alarmes marquées pour activation, et désactive les alarmes marquées pour désactivation. Les journaux correspondants sont stockés dans le groupe de `/aws/lambda/AMSAlarmSuppressor` journaux.

Gestion des journaux dans AMS Accelerate

AMS Accelerate configure les AWS services pris en charge pour collecter les journaux. Ces journaux sont utilisés par AMS Accelerate pour garantir la conformité et l'audit des ressources de votre compte.

AMS Accelerate fournit une gamme de services opérationnels pour vous aider à atteindre l'excellence opérationnelle sur AWS. Pour comprendre rapidement comment AMS aide vos équipes à atteindre l'excellence opérationnelle globale dans le cloud AWS grâce à certaines de nos principales fonctionnalités opérationnelles, notamment le service d'assistance 24 h/24, 7 j/7, la surveillance proactive, la sécurité, l'application de correctifs, la journalisation et la sauvegarde, consultez les diagrammes d'architecture de référence AMS.

Rubriques

- Gestion des journaux — AWS CloudTrail
- Gestion des journaux — Amazon EC2
- Gestion des journaux — Amazon VPC Flow Logs

Gestion des journaux — AWS CloudTrail

AWS CloudTrailest un service utilisé pour la gouvernance des comptes : conformité, audit opérationnel et audit des risques. Vous pouvez ainsi enregistrer, surveiller en permanence et conserver l'activité du compte liée aux actions menées au sein de votre AWS infrastructure. CloudTrail

AMS Accelerate nécessite une AWS CloudTrail connexion pour gérer les audits et la conformité de toutes les ressources de votre compte. Lors de l'intégration, vous pouvez choisir l'une des options suivantes :

- Piste déployée par AMS : si vous choisissez cette option, AMS crée, déploie et gère une piste CloudTrail multirégionale dans votre AWS région principale, indépendamment des pistes existantes dans votre compte.
- Proposez votre propre parcours : si vous choisissez de fournir le suivi de votre propre compte ou de votre organisation CloudTrail, vous devez travailler avec votre architecte cloud (CA) pour vous assurer qu'il répond aux configurations requises pour Accelerate. Si vous choisissez cette option mais que vous ne fournissez pas votre propre trace, Accelerate déploie automatiquement sa propre

CloudTrail trace pour garantir une sécurité continue et une couverture d'audit. Si vous fournissez votre propre piste ultérieurement, AMS supprime sa piste déployée pour éviter les redondances et les coûts supplémentaires. Cette approche permet de conserver une CloudTrail trace active unique dans votre compte et d'éviter les coûts de journalisation dupliqués.

> **Note**
>
> Si votre compte possède un suivi existant CloudTrail et que vous n'avez pas spécifiquement configuré ou demandé un suivi géré par AMS lors de l'intégration, AMS Accelerate supprime automatiquement le journal déployé AMS de votre compte. Cela permet d'éviter la double journalisation, d'optimiser l'utilisation des ressources et de réduire les coûts supplémentaires.

AMS Accelerate crée un compartiment Amazon S3 pour un journal déployé CloudTrail Accelerate en tant que destination de diffusion des événements et utilise le chiffrement AWS Key Management Service (AWS KMS). Les opérateurs d'AMS Accelerate accèdent à vos événements de randonnée à des fins d'investigation et de diagnostic. Si un suivi existant CloudTrail est déjà activé sur le compte, ce suivi s'ajoute à cela, si vous avez choisi de demander à Accelerate de déployer un suivi géré par Accelerate lors de l'intégration.

AMS Accelerate déploie des AWS Config règles pour garantir que les traces de votre CloudTrail compte, y compris une CloudTrail trace déployée par Accelerate, sont correctement configurées et cryptées. Pour en savoir plus, veuillez consulter la section AWS Config. Voici les règles utilisées, présentées sous forme de liens vers la AWS documentation qui les décrit :

- multi-region-cloudtrail-enabled. Vérifie qu'AMS Accelerate CloudTrail est correctement configuré avec les bonnes configurations.
- cloud-trail-encryption-enabled. Vérifie qui AWS CloudTrail est configuré pour utiliser le chiffrement côté serveur (SSE) avec le chiffrement par clé principale AWS KMS du client (CMK).
- cloud-trail-log-file-activé pour la validation. Lorsque cette option est activée, vérifie qu'un fichier de résumé signé contenant des journaux est AWS CloudTrail créé. Nous vous recommandons vivement d'activer la validation des fichiers sur tous les sentiers.
- s3- bucket-default-lock-enabled. Lorsque cette option est activée, vérifie que le verrouillage du compartiment Amazon S3 est activé.
- s3- bucket-logging-enabled. Lorsque cette option est activée, vérifie si la journalisation est activée pour les compartiments Amazon S3.

AMS Accelerate AWS KMS crypte les événements enregistrés pour un suivi déployé par Accelerate CloudTrail sur votre compte. Cette clé est contrôlée et accessible aux administrateurs du compte, aux opérateurs AMS Accelerate et CloudTrail. Pour plus d'informations sur les AWS Key Management Service fonctionnalités AWS KMS, consultez la documentation du produit.

Accès aux CloudTrail journaux et audit

CloudTrail les journaux d'un suivi déployé CloudTrail d'AMS Accelerate sont stockés dans un compartiment Amazon S3 au sein de votre compte. Les données de suivi stockées dans le compartiment Amazon S3 sont chiffrées à l'aide d'une clé AWS KMS créée lors du provisionnement CloudTrail des ressources.

Les compartiments Amazon S3 utilisent le modèle de dénomination ams-a ***aws account id*** -cloudtrail- (exemple : ams-a123456789- ***AWS Region*** cloudtrail-us-east -1a) et tous les événements sont stockés avec le préfixe AWS/. CloudTrail Tous les accès au compartiment principal sont enregistrés et les objets du journal sont chiffrés et versionnés à des fins d'audit.

Pour plus d'informations sur le suivi des modifications et l'interrogation des journaux, consultezSuivi des modifications apportées à vos comptes AMS Accelerate.

Protection et conservation CloudTrail des journaux

AMS Accelerate permet de verrouiller les objets Amazon S3 avec le mode de gouvernance pour un suivi déployé CloudTrail par Accelerate afin de garantir que les utilisateurs ne peuvent pas remplacer ou supprimer une version d'objet ou modifier ses paramètres de verrouillage sans autorisations spéciales. Pour plus d'informations, consultez la section Verrouillage d'objets Amazon S3.

Par défaut, tous les journaux de ce compartiment sont conservés indéfiniment. Si vous souhaitez modifier la période de conservation, vous pouvez soumettre une demande de service via le AWS Support Centre pour configurer une politique de conservation différente.

Accès aux EC2 journaux Amazon

Vous pouvez accéder aux journaux des EC2 instances Amazon en utilisant le AWS Management Console. Les journaux produits par les instances et les AWS services sont disponibles dans CloudWatch Logs, qui est disponible dans chaque compte géré par AMS Accelerate. Pour plus d'informations sur l'accès à vos journaux, consultez la documentation sur CloudWatch les journaux.

Conservation des EC2 journaux Amazon

Les journaux des EC2 instances Amazon sont conservés indéfiniment, par défaut. Si vous souhaitez modifier la période de conservation, vous pouvez soumettre une demande de service via le AWS Support Centre pour configurer une politique de conservation différente.

Gestion des journaux — Amazon EC2

AMS Accelerate installe l' CloudWatch agent sur toutes les EC2 instances Amazon que vous avez identifiées comme étant gérées par AMS Accelerate. Cet agent envoie des journaux au niveau du système à Amazon CloudWatch Logs. Pour plus d'informations, consultez Qu'est-ce qu'Amazon CloudWatch Logs ?

Les fichiers journaux suivants sont envoyés à CloudWatch Logs, dans un groupe de journaux portant le même nom que le journal. Au sein de chaque groupe de journaux, un flux de journal est créé pour chaque EC2 instance Amazon, nommé en fonction de l'ID d' EC2 instance Amazon.

Linux

- /var/log/amazon/ssm/amazon-ssm-agent.log
- /var/log/amazon/ssm/errors.journal
- /var/log/audit/audit.journal
- /var/log/auth.journal
- /var/log/cloud-init-output.log
- /var/log/cron
- /var/log/dnf.journal
- /var/log/dpkg.journal
- /var/log/maillog
- /var/log/messages
- /var/log/secure
- /var/log/spooler
- /var/log/syslog
- /var/log/yum.journal
- /var/log/zypper.journal

Pour plus d'informations, voir Création ou modification manuelle du fichier de configuration de l' CloudWatch agent.

Windows

- SSMAgentJournal Amazon
- AmazonCloudWatchAgentLog
- SSMErrorJournal Amazon
- AmazonCloudFormationLog
- ApplicationEventLog
- EC2ConfigServiceEventLog
- MicrosoftWindowsAppLockerEXEAndDLLEventJournal
- MicrosoftWindowsAppLockerMSIAndScriptEventLog
- MicrosoftWindowsGroupPolicyOperationalEventLog
- SecurityEventLog
- SystemEventLog

Pour plus d'informations, consultez Démarrage rapide : activez vos EC2 instances Amazon exécutant Windows Server 2016 pour envoyer des journaux à des CloudWatch journaux à l'aide de l'agent CloudWatch Logs.

Gestion des journaux — Amazon VPC Flow Logs

Les journaux de flux VPC sont une fonctionnalité qui capture des informations sur le trafic IP à destination et en provenance des interfaces réseau de votre VPC. Les données des journaux de flux peuvent être publiées sur Amazon CloudWatch Logs ou Amazon S3. La collecte des données du journal de flux n'a aucune incidence sur le débit ou la latence du réseau. Vous pouvez créer ou supprimer des journaux de flux sans aucune incidence sur les performances du réseau.

Les journaux de flux peuvent vous aider pour de nombreuses tâches, par exemple :

- Diagnostic des règles trop restrictives des groupes de sécurité
- Surveillance du trafic qui atteint votre instance
- Déterminer la direction du trafic vers et depuis les interfaces réseau

Il n'est pas nécessaire d'activer les journaux de flux VPC pour chaque VPC nouvellement créé dans les comptes Accelerate. AMS détectera automatiquement si un VPC possède un journal de flux à l'aide de la règle - ams-nist-cis-vpcflow-logs-enabledConfig. Si les journaux de flux VPC ne sont pas activés, AMS y remédiera automatiquement en créant un journal de flux VPC avec des champs personnalisés. Ces champs supplémentaires permettront à AMS et à ses clients de mieux surveiller le trafic VPC, de comprendre les dépendances du réseau, de résoudre les problèmes de connectivité réseau et d'identifier les menaces réseau.

Pour plus d'informations sur l'affichage et la recherche dans les journaux de flux, voir Utilisation des journaux de flux.

Suivi des modifications apportées à vos comptes AMS Accelerate

Important

Le service Change Record est obsolète depuis le 1er juillet 2025.
Les nouveaux comptes ne peuvent pas être intégrés au service Change Record.
Pour interroger CloudTrail les données de vos comptes AMS Accelerate, vous pouvez utiliser les services suivants :

- Dans AWS CloudTrail, choisissez Historique des événements et filtrez les événements à l'aide des attributs de recherche. Vous pouvez utiliser le filtre par plage de temps et choisir de filtrer l'historique des événements par source d'événement en `s3.amazon.aws.com` spécifiant, ou choisir de filtrer l'historique des événements par nom d'utilisateur. Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements.
- Utilisez AWS CloudTrail Lake pour recueillir des données par le biais de requêtes. Dans, AWS CloudTrail choisissez Lake, puis Query. Vous pouvez créer vos propres requêtes, utiliser le générateur de requêtes ou utiliser des exemples de requêtes pour recueillir des données basées sur des événements. Par exemple, vous pouvez demander qui a supprimé une EC2 instance Amazon la semaine dernière. Pour plus d'informations, consultez la section Création d'un lac de données à partir d'une AWS CloudTrail source et de CloudTrailLake requêtes.
- Créez une table Amazon Athena AWS CloudTrail et définissez l'emplacement de stockage comme étant le compartiment Amazon S3 associé à votre parcours. Vérifiez que la région d'origine de votre sentier et celle du compartiment Amazon S3 sont identiques. Dans Amazon Athena, utilisez l'éditeur de requêtes pour exécuter les requêtes par défaut fournies par Accelerate à utiliser avec la console Athena. Pour plus d'informations sur la création d'une table Athena pour interroger les CloudTrail journaux, consultez la section Journaux des requêtes AWS CloudTrail.

Rubriques

- Afficher vos enregistrements de modifications
- Requêtes par défaut
- Modifier les autorisations d'enregistrement

AWS Managed Services vous aide à suivre les modifications apportées par l'équipe AMS Accelerate Operations et AMS Accelerate Automation en fournissant une interface interrogeable à l'aide de la console Amazon Athena (Athena) et de la gestion des journaux AMS Accelerate.

Athena est un service de requête interactif que vous pouvez utiliser pour analyser des données dans Amazon S3 à l'aide du langage de requête structuré (SQL) standard (voir Référence SQL pour Amazon Athena). Athena fonctionnant sans serveur, vous n'avez pas d'infrastructure à gérer et vous ne payez que pour les requêtes que vous exécutez. AMS Accelerate crée des tables Athena avec des partitions quotidiennes sur les CloudTrail journaux, et fournit des requêtes sur votre AWS région principale et au sein du ams-change-recordgroupe de travail. Vous pouvez choisir n'importe laquelle des requêtes par défaut et les exécuter selon vos besoins. Pour en savoir plus sur les groupes de travail Athena, consultez Comment fonctionnent les groupes de travail.

> **Note**
>
> Seul Accelerate peut interroger les CloudTrail événements de votre compte Accelerate à l'aide d'Athena lorsqu'Accelerate est intégré au journal de votre CloudTrail organisation, sauf si l'administrateur de votre organisation a déployé un rôle IAM pour utiliser Athena pour interroger et analyser les CloudTrail événements de votre compte, lors de l'intégration.

À l'aide de l'enregistrement des modifications, vous pouvez facilement répondre à des questions telles que :

- Qui (AMS Accelerate Systems ou AMS Accelerate Operators) a accédé à votre compte
- Quelles modifications ont été apportées par AMS Accelerate à votre compte ?
- Quand est-ce qu'AMS Accelerate a apporté des modifications à votre compte ?
- Où consulter les modifications apportées à votre compte
- Pourquoi AMS Accelerate avait besoin d'apporter les modifications à votre compte
- Comment modifier les requêtes pour obtenir des réponses à toutes ces questions, y compris pour toute modification non liée à l'AMS

Afficher vos enregistrements de modifications

Pour utiliser les requêtes Athena, connectez-vous à la console de AWS gestion et accédez à la console Athena dans votre région principale. AWS

> **Note**
>
> Si la page de démarrage d'Amazon Athena s'affiche lorsque vous effectuez l'une des étapes, cliquez sur Commencer. Cela peut vous apparaître même si votre infrastructure d'enregistrement des modifications est déjà en place.

1. Choisissez Workgroup dans le panneau de navigation supérieur de la console Athena.
2. Choisissez le ams-change-recordgroupe de travail, puis cliquez sur Changer de groupe de travail.
3. Choisissez dans la zone ams-change-record-databasede liste déroulante de base de données. Le ams-change-record-tabletableau est ams-change-record-databaseinclus.
4. Choisissez Requêtes enregistrées dans le panneau de navigation supérieur.
5. La fenêtre Requêtes enregistrées affiche la liste des requêtes fournies par AMS Accelerate, que vous pouvez exécuter. Choisissez la requête que vous souhaitez exécuter dans la liste des requêtes enregistrées. Par exemple, requête ams_session_accesses_v1.

   Pour la liste complète des requêtes AMS Accelerate prédéfinies, voirRequêtes par défaut.
6. Ajustez le filtre date/heure dans la boîte de l'éditeur de requête selon vos besoins ; par défaut, la requête ne vérifie que les modifications effectuées depuis le dernier jour.
7. Choisissez Exécuter la requête.

Requêtes par défaut

AMS Accelerate fournit plusieurs requêtes par défaut que vous pouvez utiliser dans la console Athena. Les requêtes par défaut sont répertoriées dans les tableaux suivants.

> **Note**
>
> - Toutes les requêtes acceptent la plage de dates et d'heures comme filtre facultatif ; par défaut, toutes les requêtes sont exécutées au cours des dernières 24 heures. Pour les informations attendues, voir la sous-section suivante,Modification du filtre date/heure dans les requêtes.
> - Les entrées de paramètres que vous pouvez ou devez modifier sont affichées dans la requête sous forme *<PARAMETER_NAME>* d'accolades angulaires. Remplacez l'espace réservé et les accolades angulaires par la valeur de votre paramètre.

- Tous les filtres sont facultatifs. Dans les requêtes, certains filtres facultatifs sont commentés par un double tiret (--) au début de la ligne. Toutes les requêtes seront exécutées sans eux, avec les paramètres par défaut. Si vous souhaitez définir des valeurs de paramètres pour ces filtres facultatifs, supprimez le double tiret (--) au début de la ligne et remplacez le paramètre comme vous le souhaitez.
- Toutes les requêtes renvoient `IAM PincipalId` et `IAM SessionId` apparaissent dans les sorties
- Le coût calculé pour exécuter une requête dépend du nombre de CloudTrail journaux générés pour le compte. Pour calculer le coût, utilisez le calculateur de prix AWS Athena.

Requêtes prédéfinies

Objet/Description	Inputs	Outputs
Nom de la requête : `ams_access_session_query_v1`		
Suivi des sessions d'accès AMS Accelerate Fournit des informations sur une session d'accès AMS Accelerate spécifique. La requête accepte l'ID principal IAM comme filtre facultatif et renvoie l'heure de l'événement, les besoins commerciaux pour accéder au compte, le demandeur, etc. Vous pouvez filtrer en fonction d'un ID principal IAM spécifique en décommentant la ligne et en remplaçant l'espace réservé *`IAM Principal Id`* par un identifiant	(Facultatif) `IAM PrincipalId` : Identifiant principal IAM de la ressource qui tente d'accéder. Le format est *`UNIQUE_ID ENTIFIER :RESOURCE_NAME`* . Pour plus de détails, voir Identifiants uniques. Vous pouvez exécuter la requête sans ce filtre pour déterminer l'IAM PrincipalId exact avec lequel vous souhaitez filtrer.	• EventTime: Heure d'obtention de l'accès • EventName: nom de l'événement AWS (AssumeRole) • EventRegion: région AWS qui reçoit la demande • EventId: ID de CloudTrail l'événement • BusinessNeed Type : type de raison commerciale pour accéder au compte. Les valeurs autorisées sont : SupportCase OpsItem, Issue, Text. • BusinessNeed: Les entreprises doivent accéder au compte. Par exemple, l'identifiant du dossier de support, l'identifiant de l'élément opérationnel, etc. • Demandeur : ID de l'opérateur qui accède au compte ou système

Objet/Description	Inputs	Outputs
spécifique dans l'éditeur de requêtes. Vous pouvez également répertorier les sessions d'accès non-AMS en supprimant la ligne de filtre useragent dans la clause WHERE de la requête.		d'automatisation qui accède au compte. • RequestAccessType: type de demandeur (System, OpsAPI OpsConsole, Unset)
Nom de la requête : `ams_events_query_v1`		
Suivez toutes les actions de mutation effectuées par AMS Accelerate Renvoie toutes les actions d'écriture effectuées sur le compte à l'aide de ce filtre de rôle AMS Accelerate. Vous pouvez également suivre les actions de mutation effectuées par des rôles non-AMS en supprimant les lignes de filtre useridentity.arn de la clause WHERE de la requête.	(Facultatif) Seule la plage de dates et d'heures. Consultez Modification du filtre date/heure dans les requêtes.	• AccountId: ID de compte AWS • RoleArn: RoleArn pour le demandeur • EventTime: Heure d'obtention de l'accès • EventName: nom de l'événement AWS (AssumeRole) • EventRegion: région AWS qui reçoit la demande • EventId: ID de CloudTrail l'événement • RequestParameters : paramètres de demande pour la demande • ResponseElements: éléments de réponse pour la réponse. • UserAgent: agent CloudTrail utilisateur AWS
Nom de la requête : `ams_instance_access_sessions_query_v1`		

Objet/Description	Inputs	Outputs
Suivez les accès aux instances par AMS Accelerate Renvoie une liste des accès aux instances AMS Accelerate ; chaque enregistrement inclut l'heure de l'événement, la région de l'événement, l'ID d'instance, l'ID principal IAM, l'ID de session IAM, l'ID de session SSM. Vous pouvez utiliser l'ID principal IAM pour obtenir plus de détails sur les besoins de l'entreprise en matière d'accès à l'instance à l'aide de la requête `ams_access_sessions_query_v1` Athena. Vous pouvez utiliser l'ID de session SSM pour obtenir plus de détails sur la session d'accès à l'instance, notamment l'heure de début et de fin de la session, les détails du journal et l'utilisation de la console du gestionnaire de AWS session dans la AWS région de l'instance.	Seul `datetime range`. Consultez Modification du filtre date/heure dans les requêtes.	• InstanceId: ID de l'instance • SSMSession Identifiant : ID de session SSM • RoleArn: RoleArn pour le demandeur • EventTime: Heure d'obtention de l'accès • EventName: nom de l'événement AWS (AssumeRole) • EventRegion: région AWS qui reçoit la demande • EventId: ID de CloudTrail l'événement

Objet/Description	Inputs	Outputs
Les utilisateurs peuvent également répertorier les accès aux instances non AMS en supprimant la ligne de filtre useridentity dans la clause WHERE de la requête.		

Nom de la requête : `ams_privilege_escalation_events_query_v1`

Objet/Description	Inputs	Outputs
Suivez les événements relatifs aux autorisations (escalade) pour les utilisateurs AMS et non-AMS Fournit une liste d'événements susceptibles d'entraîner directement ou potentiellement une augmentation des privilèges. La requête accepte ActionedBy comme filtre facultatif et renvoie EventName, EventId EventTime, et ainsi de suite. Tous les champs associés à l'événement sont également renvoyés. Les champs sont vides s'ils ne s'appliquent pas à cet événement. Le ActionedBy filtre est désactivé par défaut ; pour l'activer, supprimez « -- » de cette ligne. Par défaut, le ActionedBy filtre est désactivé (il affiche les événements d'augmentation de privilèges de tous les utilisateurs). Pour afficher les événements relatifs à	(Facultatif) `ACTIONEDBY_PUT_USER_NAME` : nom d'utilisateur de l'utilisateur ActionedBy. Il peut s'agir d'un utilisateur ou d'un rôle IAM. Par exemple, ams-access-admin. (Facultatif) `datetime range`. Consultez Modification du filtre date/heure dans les requêtes.	• AccountId: ID de compte • ActionedBy: ActionedBy Nom d'utilisateur • EventTime: Heure d'obtention de l'accès • EventName: nom de l'événement AWS (AssumeRole). • EventRegion: région AWS qui reçoit la demande • EventId: ID de CloudTrail l'événement

Objet/Description	Inputs	Outputs
un utilisateur ou à un rôle en particulier, supprimez le double tiret (--) de la ligne de filtre useridentity dans la clause WHERE et remplacez l'espace réservé par un nom *ACTIONEDBY_PUT_USER_NAME_HERE* d'utilisateur ou de rôle IAM. Vous pouvez exécuter la requête sans le filtre pour déterminer l'utilisateur exact avec lequel vous souhaitez filtrer.		
Nom de la requête : `ams_resource_events_query_v1`		

Objet/Description	Inputs	Outputs
Suivez les événements de rédaction pour des ressources spécifiques (AMS ou non-AMS) Fournit une liste des événements effectués sur une ressource spécifique. La requête accepte l'ID de ressource dans les filtres (remplacez l'espace réservé *RESOURCE_INFO* dans la clause WHERE de la requête) et renvoie toutes les actions d'écriture effectuées sur cette ressource.	(Obligatoire) `RESOURCE_INFO` : L'identifiant de ressource peut être un identifiant pour n'importe quelle ressource AWS du compte. Ne confondez pas cela avec les ressources ARNs. Par exemple, un ID d'instance pour une EC2 instance, un nom de table pour une table DynamoDB logGroupName , pour CloudWatch un journal, etc. (Facultatif) `datetime range`. Consultez Modification du filtre date/heure dans les requêtes.	• AccountId: ID de compte • ActionedBy: ActionedBy Nom d'utilisateur • EventTime: Heure d'obtention de l'accès • EventName: nom de l'événement AWS (AssumeRole). • EventRegion: région AWS qui reçoit la demande • EventId: ID de CloudTrail l'événement
Nom de la requête : `ams_session_events_query_v1`		

Objet/Description	Inputs	Outputs
Suivez les actions d'écriture effectuées par AMS Accelerate au cours d'une session spécifique Fournit une liste des événements réalisés au cours d'une session spécifique. La requête accepte l'ID principal IAM dans le cadre des filtres (remplacez l'espace réservé *PRINCIPAL_ID* dans la clause WHERE de la requête) et renvoie toutes les actions d'écriture effectuées sur cette ressource.	(Obligatoire) `PRINCIPAL_ID` : ID principal de la session. Le format est *UNIQUE_ID ENTIFIER* :*RESOURCE_NAME* . Pour plus de détails, voir Identifiants uniques. Vous pouvez exécuter la requête « ams_session_ids_by_requester_v1" pour obtenir la liste des principaux IAM d'un demandeur. IDs Vous pouvez également exécuter la requête sans ce filtre pour déterminer l'IAM exact avec Principal Id lequel vous souhaitez filtrer. (Facultatif) `datetime range`. Consultez Modification du filtre date/heure dans les requêtes.	• AccountId: ID de compte • ActionedBy: ActionedBy Nom d'utilisateur • EventTime: Heure d'obtention de l'accès • EventName: nom de l'événement AWS (AssumeRole) • EventRegion: région AWS qui reçoit la demande • EventId: ID de CloudTrail l'événement
Nom de la requête : `ams_session_ids_by_requester_v1`		

Objet/Description	Inputs	Outputs
Suivez l'IAM Principal /Session IDs pour un demandeur spécifique. La requête accepte le terme « demandeur » (remplacez l'espace réservé *Requester* dans la clause WHERE de la requête) et renvoie tous les identifiants principaux IAM de ce demandeur pendant la période spécifiée.	(Obligatoire) `Requester` : ID d'opérateur qui accède au compte (par exemple : alias d'un opérateur), ou système d'automatisation qui accède au compte (par exemple : OsConfiguration, AlarmManager, etc.). (Facultatif) `datetime range`. Consultez Modification du filtre date/heure dans les requêtes.	• IAM PrincipalId - Identifiant principal IAM de la session. Le format est *UNIQUE_IDENTIFIER* :*RESOURCE_NAME* . Pour plus de détails, voir Identifiants uniques. Vous pouvez exécuter la requête sans ce filtre pour déterminer l'IAM exact avec Principal Id lequel vous souhaitez filtrer. • IAM SessionId - ID de session IAM pour la session d'accès • EventTime: Heure d'obtention de l'accès

Modification du filtre date/heure dans les requêtes

Toutes les requêtes acceptent la plage de dates et d'heures comme filtre facultatif. Par défaut, toutes les requêtes sont exécutées au cours du dernier jour.

Le format utilisé pour le champ datetime est yyyy/MM/dd (par exemple : 01/01/2021). N'oubliez pas qu'il ne stocke que la date et non l'horodatage complet. Pour l'horodatage complet, utilisez le champ eventime, qui stocke l'horodatage au format ISO 8601 yyyy-MM-dd T HH:mm:SS Z (par exemple : 2021-01-01T 23:59:59 Z). Cependant, étant donné que la table est partitionnée dans le champ datetime, vous devez transmettre le filtre datetime et eventtime à la requête. Voir les exemples suivantes.

> **Note**
>
> Pour voir toutes les manières acceptées de modifier la plage, consultez la dernière documentation des fonctions Presto basée sur la version du moteur Athena actuellement utilisée pour les fonctions et les opérateurs de date et d'heure pour voir toutes les méthodes acceptées pour modifier la plage.

Niveau de date : 1 dernier jour ou dernières 24 heures (par défaut) Exemple : si CURRENT_DATE='2021/01/01', le filtre soustraira un jour de la date actuelle et le formatera comme date/heure > '2020/12/31'

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
```

Niveau de date : exemple des 2 derniers mois :

```
datetime > date_format(date_add('month', - 2, CURRENT_DATE), '%Y/%m/%d')
```

Niveau de date : entre 2 dates, exemple :

```
datetime > '2021/01/01'
      AND
      datetime < '2021/01/10'
```

Niveau d'horodatage : exemple des 12 dernières heures :

Partitionnez les données numérisées pour qu'elles durent 1 jour, puis filtrez tous les événements survenus au cours des 12 dernières heures

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND
      eventtime > date_format(date_add('hour', - 12, CURRENT_TIMESTAMP), '%Y-%m-%dT%H:
%i:%sZ')
```

Niveau d'horodatage : entre 2 horodatages, exemple :

Organisez des événements entre le 1er janvier 2021 à 12 h 00 et le 10 janvier 2021 à 15 h 00.

```
datetime > '2021/01/01' AND datetime < '2021/01/10'
      AND
      eventtime > '2021-01-01T12:00:00Z' AND eventtime < '2021-01-10T15:00:00Z'
```

Exemples de requêtes par défaut

ams_access_session_query_v1

```
Name: ams_access_session_query_v1

Description: >-
```

```
    The query provides more information on specific AMS access session.
    The query accepts IAM Principal Id as an optional filter and returns event time,
  business need for accessing the account, requester, ... etc.
    By default; the query filter last day events only, the user can change the datetime
  filter to search for more wide time range.
    By default; the IAM PrincipalId filter is disabled. To enable it, remove "-- " from
  that line.

AthenaQueryString: |-
    /*
      The query provides list of AMS access sessions during specific time range.
      The query accepts IAM Principal Id as an optional filter and returns event time,
  business need for accessing the account, requester, ... etc.

      By default, the query filters the last day's events only; you can change the
  "datetime" filter to search for a wider time range.

      By default; the IAM Principal ID filter is disabled (it shows access sessions for
  all IAM principals).
      If you want to only show access sessions for a particular IAM principal ID, remove
  the double-dash (--) from
      the "IAM Principal ID" filter line in the WHERE clause of the query, and replace
  the placeholder "<IAM PrincipalId>" with the specific ID that you want.
      You can run the query without the filter to determine the exact IAM PrincipalId
  you want to filter with.

      By default; the query only shows AMS access sessions. If you also want to show
  non-AMS access sessions,
      remove the "useragent" filter in the WHERE clause of the query.

      For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
  in your AMS Accelerate accounts -> Default Queries
    */

    SELECT
       json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
  PrincipalId",
       json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
  SessionId",
       eventtime AS "EventTime",
       eventname AS "EventName",
       awsregion AS "EventRegion",
       eventid AS "EventId",
       json_extract_scalar(requestparameters, '$.tags[0].value') AS "BusinessNeed",
```

```
      json_extract_scalar(requestparameters, '$.tags[1].value') AS "BusinessNeedType",
      json_extract_scalar(requestparameters, '$.tags[2].value') AS "Requester",
      json_extract_scalar(requestparameters, '$.tags[3].value') AS "AccessRequestType"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND eventname = 'AssumeRole'
      AND useragent = 'access.managedservices.amazonaws.com'
      -- AND  json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId')
 = '<IAM PrincipalId>'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of AMS access sessions during specific time range.
   # The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.
   #
   # By default; the IAM Principal ID filter is disabled (it shows access sessions for
 all IAM principals).
   # If you want to only show access sessions for a particular IAM principal ID, remove
 the # (#) from
   # the "IAM Principal ID" filter of the query, and replace the placeholder "<IAM
 PrincipalId>" with the specific ID that you want.
   # You can run the query without the filter to determine the exact IAM PrincipalId
 you want to filter with.
   #
   # By default; the query only shows AMS access sessions. If you also want to show
 non-AMS access sessions,
   # remove the "useragent" filter from the query.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter eventName="AssumeRole" AND userAgent="access.managedservices.amazonaws.com"
   # | filter responseElements.assumedRoleUser.assumedRoleId= "<IAM PrincipalId>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
      responseElements.credentials.accessKeyId as IAMSessionId,
      eventTime as EventTime,
      eventName as EventName,
      awsRegion as EventRegion,
      eventID as EventId,
```

```
      requestParameters.tags.0.value as BusinessNeed,
      requestParameters.tags.1.value as BusinessNeedType,
      requestParameters.tags.2.value as Requester,
      requestParameters.tags.3.value as AccessRequestType
```

ams_events_query_v1

```
ams_events_query_v1.yaml
/*
  The query provides list of events to track write actions for all AMS changes.
  The query returns all write actions done on the account using that AMS role filter.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  You can also track mutating actions done by non-AMS roles by removing the
 "useridentity.arn" filter lines from the WHERE clause of the query.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   useridentity.arn AS "RoleArn",
   eventid AS "EventId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventsource AS "EventService",
   eventtime AS "EventTime",
   requestparameters As "RequestParameters",
   responseelements AS "ResponseElements",
   useragent AS "UserAgent"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   readonly <> 'true'
   AND
   (
      LOWER(useridentity.arn) LIKE '%/ams%'
```

```
      OR LOWER(useridentity.arn) LIKE '%/customer_ssm_automation_role%'
   )
ORDER BY eventtime
```

ams_instance_access_sessions_query_v1

```
ams_instance_access_sessions_query_v1
/*
  The query provides list of AMS Instance accesses during specific time range.

  The query returns the list of AMS instance accesses; every record includes the event
 time, the event AWS Region, the instance ID, the IAM session ID, and the SSM session
 ID.
  You can use the IAM Principal ID to get more details on the business need for
 accessing the instance by using ams_access_session_query_v1 athena query.
  You can use the SSM session ID to get more details on the instance access session,
 including the start and end time of the session and log details, using the AWS Session
 Manager Console in the instance's AWS Region.

  You can also list non-AMS instance accesses by removing the "useridentity" filter
 line in the WHERE clause of the query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   json_extract_scalar(requestparameters, '$.target') AS "InstanceId",
   json_extract_scalar(responseelements, '$.sessionId') AS "SSM SessionId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventsource AS "EventService",
   eventtime AS "EventTime"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   useridentity.sessionContext.sessionIssuer.arn like '%/ams_%'
```

```
   AND eventname = 'StartSession'
ORDER BY eventtime
```

ams_privilege_escalation_events_query_v1

```
ams_privilege_escalation_events_query_v1.yaml
/*
  The query provides list of events that can directly or potentially lead to a
 privilege escalation.

  The query accepts ActionedBy as an optional filter and returns EventName, EventId,
 EventTime, ... etc.
  All fields associated with the event are also returned. Some fields are blank if not
 applicable for that event.
  You can use the IAM Session ID to get more details about events happened in that
 session by using ams_session_events_query_v1 query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  By default, the ActionedBy filter is disabled (it shows privilege escalation events
 from all users).
  To show events for a particular user or role, remove the double-dash (--) from the
 useridentity filter line in the WHERE clause of the query
  and replace the placeholder "<ACTIONEDBY_PUT_USER_NAME_HERE>" with an IAM user or
 role name.
  You can run the query without the filter to determine the exact user you want to
 filter with.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventtime AS "EventTime",
   json_extract_scalar(requestparameters, '$.userName') AS "UserName",
```

```
   json_extract_scalar(requestparameters, '$.roleName') AS "RoleName",
   json_extract_scalar(requestparameters, '$.groupName') AS "GroupName",
   json_extract_scalar(requestparameters, '$.policyArn') AS "PolicyArn",
   json_extract_scalar(requestparameters, '$.policyName') AS "PolicyName",
   json_extract_scalar(requestparameters, '$.permissionsBoundary') AS
 "PermissionsBoundary",
   json_extract_scalar(requestparameters, '$.instanceProfileName') AS
 "InstanceProfileName",
   json_extract_scalar(requestparameters, '$.openIDConnectProviderArn') AS
 "OpenIDConnectProviderArn",
   json_extract_scalar(requestparameters, '$.serialNumber') AS "SerialNumber",
   json_extract_scalar(requestparameters, '$.serverCertificateName') AS
 "ServerCertificateName",
   json_extract_scalar(requestparameters, '$.accessKeyId') AS "AccessKeyId",
   json_extract_scalar(requestparameters, '$.certificateId') AS "CertificateId",
   json_extract_scalar(requestparameters, '$.newUserName') AS "NewUserName",
   json_extract_scalar(requestparameters, '$.newGroupName') AS "NewGroupName",
   json_extract_scalar(requestparameters, '$.newServerCertificateName') AS
 "NewServerCertificateName",
   json_extract_scalar(requestparameters, '$.name') AS "SAMLProviderName",
   json_extract_scalar(requestparameters, '$.sAMLProviderArn') AS "SAMLProviderArn",
   json_extract_scalar(requestparameters, '$.sSHPublicKeyId') AS "SSHPublicKeyId",
   json_extract_scalar(requestparameters, '$.virtualMFADeviceName') AS
 "VirtualMFADeviceName"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   (
     -- More event names can be found at https://docs.aws.amazon.com/IAM/latest/
UserGuide/list_identityandaccessmanagement.html
     eventname LIKE 'Add%' OR
     eventname LIKE 'Attach%' OR
     eventname LIKE 'Delete%' AND eventname != 'DeleteAccountAlias' OR
     eventname LIKE 'Detach%' OR
     eventname LIKE 'Create%' AND eventname != 'CreateAccountAlias' OR
     eventname LIKE 'Put%' OR
     eventname LIKE 'Remove%' OR
     eventname LIKE 'Update%' OR
     eventname LIKE 'Upload%' OR
     eventname = 'DeactivateMFADevice' OR
     eventname = 'EnableMFADevice' OR
     eventname = 'ResetServiceSpecificCredential' OR
     eventname = 'SetDefaultPolicyVersion'
   )
```

```
   AND eventsource = 'iam.amazonaws.com'
ORDER BY eventtime
```

ams_resource_events_query_v1

```
Name: ams_resource_events_query_v1

Description: >-
   The query provides list of events done on specific resource.
   The query accepts resource id as part of the filters, and return all write actions
 done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of events done on specific resource.

     The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the WHERE clause of the query),
     and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
     Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventid AS "EventId",
      eventsource AS "EventService",
      eventtime AS "EventTime"
   FROM
```

```
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
      AND
      (
         requestparameters LIKE '%<RESOURCE_INFO>%'
         OR responseelements LIKE '%<RESOURCE_INFO>%'
      )
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of events done on specific resource.
   #
   # The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the filter of the query),
   # and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
   # Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
   # | filter RequestParameters like "RESOURCE_INFO" or ResponseElements like
 "<RESOURCE_INFO>"
   | fields
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
      awsRegion as EventRegion,
      eventID as EventId,
      eventSource as EventService,
      eventTime as EventTime
   | display IAMPrincipalId, IAMSessionId, AccountId, ActionedBy, EventName,
 EventRegion, EventId, EventService, EventTime
   | sort eventTime desc
```

ams_session_events_query_v1

```
Name: ams_session_events_query_v1

Description: >-
   The query provides list of events done on specific session.
   The query accepts IAM Principal Id as part of the filters, and return all write
 actions done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides a list of events executed on a specific session.

     The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the WHERE clause of the query),
     and returns all write actions done on that resource.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventsource AS "EventService",
      eventtime AS "EventTime",
      requestparameters As "RequestParameters",
      responseelements AS "ResponseElements",
      useragent AS "UserAgent"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate   WHERE
      useridentity.principalid = '<PRINCIPAL_ID>'
      AND datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
   ORDER BY eventtime
```

```
InsightsQueryString: |-
   # The query provides a list of events executed on a specific session.
   #
   # The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the filter of the query),
   # and returns all write actions done on that resource.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0 AND userIdentity.principalId = "<IAM Principal>"
   | sort eventTime desc
   | fields
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
      awsRegion as EventRegion,
      eventSource as EventService,
      eventTime as EventTime,
      userAgent as UserAgent
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
```

ams_session_ids_by_requester_v1

```
Name: ams_session_ids_by_requester_v1

Description: >-
   The query provides list of IAM Principal/Session Ids for specific requester.
   The query accepts requester and return all IAM Principal/Session Ids by that
 requester during specific time range.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of IAM Principal IDs for a specific requester.

     The query accepts the requester (replace placeholder "<Requester>" in the WHERE
 clause of the query),
```

```
     and returns all IAM Principal IDs by that requester during a specific time range.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
 PrincipalId",
      json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
 SessionIId",
      eventtime AS "EventTime"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND json_extract_scalar(requestparameters, '$.tags[2].value') = '<Requester>'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of IAM Principal IDs for a specific requester.
   #
   # The query accepts the requester (replace placeholder "<Requester>" in the filter
 of the query),
   # and returns all IAM Principal IDs by that requester during a specific time range.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   filter eventName="AssumeRole" AND requestParameters.tags.2.value="<Requester>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
      responseElements.credentials.accessKeyId as IAMSessionId,
      eventTime as EventTime
```

Modifier les autorisations d'enregistrement

Les autorisations suivantes sont nécessaires pour exécuter des requêtes d'enregistrement de modification :

- Athéna
  - Athéna : GetWorkGroup
  - Athéna : StartQueryExecution
  - Athéna : ListDataCatalogs
  - Athéna : GetQueryExecution
  - Athéna : GetQueryResults
  - Athéna : BatchGetNamedQuery
  - Athéna : ListWorkGroups
  - Athéna : UpdateWorkGroup
  - Athéna : GetNamedQuery
  - Athéna : ListQueryExecutions
  - Athéna : ListNamedQueries
- AWS KMS
  - kms:Decrypt
  - AWS KMS ID clé de AMSCloudTrailLogManagement, ou votre/vos identifiant (s) AWS KMS clé (s), si Accelerate utilise vos CloudTrail événements de suivi, le magasin de données du compartiment Amazon S3 à l'aide du cryptage SSE-KMS.
- AWS Glue
  - colle : GetDatabase
  - colle : GetTables
  - colle : GetDatabases
  - colle : GetTable
- Accès en lecture à Amazon S3
  - Banque de CloudTrail données du compartiment Amazon S3 : ams-a *`AccountId`* -cloudtrail-, ou le nom de *`primary region`* votre compartiment Amazon S3, suivi des événements, magasin de données du compartiment CloudTrail Amazon S3.
- Accès en écriture sur Amazon S3
  - Résultats de la requête relative aux événements Athena, compartiment Amazon S3 : *`AccountId`* ams-a athena-results- *`primary region`*

AWS Systems Manager dans Accelerate

Un AWS Systems Manager document (document SSM) définit les actions que Systems Manager effectue sur vos AWS ressources. Systems Manager inclut plus d'une douzaine de documents préconfigurés que vous pouvez utiliser en spécifiant des paramètres lors de l'exécution. Les documents utilisent la notation d' JavaScript objet (JSON) ou YAML, et ils incluent des étapes et des paramètres que vous spécifiez.

AWS Managed Services (AMS) est un éditeur de confiance pour les documents SSM. Les documents SSM détenus par AMS sont partagés uniquement avec les comptes AMS intégrés, commencent toujours par un préfixe réservé (AWSManagedServices-*) et apparaissent dans la console Systems Manager, comme appartenant à Amazon. Le processus AMS pour le développement et la publication de documents SSM suit les meilleures pratiques d'AWS et nécessite plusieurs évaluations par les pairs tout au long du cycle de vie du document. Pour plus d'informations sur les meilleures pratiques d'AWS en matière de partage de documents SSM, consultez la page Meilleures pratiques pour les documents SSM partagés.

Documents AMS Accelerate SSM disponibles

Les documents AMS Accelerate SSM sont disponibles exclusivement pour les clients AMS Accelerate et sont utilisés pour automatiser le flux de travail opérationnel nécessaire à l'exploitation de votre compte.

Pour consulter les documents AMS Accelerate SSM disponibles sur AWS Management Console :

1. Ouvrez la console Systems Manager sur la console.AWS Systems Manager
2. Choisissez Partagé avec moi.
3. Dans la barre de recherche, filtrez par préfixe du nom du document, puis par Égaux, et définissez la valeur sur AWSManagedServices-.

   Pour AWS CLI obtenir des instructions, consultez la section Utilisation de documents SSM partagés.

Versions des documents AMS Accelerate SSM

Les documents SSM prennent en charge le contrôle de version. Les documents AMS Accelerate SSM ne peuvent pas être modifiés depuis le compte du client et ne peuvent pas être repartagés. Ils sont gérés et maintenus de manière centralisée par AMS Accelerate afin de gérer le compte.

Les numéros de version sont incrémentés à chaque mise à jour de document dans une région AWS spécifique. À mesure que de nouvelles régions sont disponibles, le même contenu de document dans deux régions peut avoir des numéros de version différents ; cela est typique et ne signifie pas que leur comportement sera différent. Si vous souhaitez comparer deux documents AMS Accelerate SSM, nous vous recommandons de comparer leurs hachages avec : AWS CLI

```
aws ssm describe-document \
--name AWSManagedServices-DOCUMENTNAME \
--output text --query "Document.Hash"
```

Deux documents SSM sont identiques si leurs hachages correspondent.

Tarification Systems Manager

L'accès aux documents AMS Accelerate SSM est gratuit. Le coût d'exécution varie en fonction du type de document SSM, de ses étapes et de la durée d'exécution. Pour plus d'informations, reportez-vous à la section AWS Systems Manager Tarification.

Historique du document pour le guide de l'utilisateur d'AMS Accelerate

Le tableau suivant décrit les modifications importantes apportées à chaque version du guide de l'utilisateur d'AMS Accelerate. Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

Modification	Description	Date
Gestion des journaux mise à jour — AWS CloudTrail section	Nouvelles informations et remarques concernant la AWS CloudTrail journalisation.	25 septembre 2025
Ajout de 4 nouveaux contrôles d'optimisation des Trusted Advisor coûts pris en charge par Trusted Remediator	Les contrôles d'optimisation des coûts suivants ont été ajoutés : • c1z7kmr00n - Recommandations d'optimisation des coûts Amazon pour les instances EC2 • c1z7kmr02n - Recommandations d'optimisation des coûts Amazon EBS pour les volumes • c1z7kmr03n - Recommandations d'optimisation des coûts Amazon RDS pour les instances de base de données • c1z7kmr05n - recommandations d'optimisation des coûts pour les fonctions AWS Lambda	22 septembre 2025

Note de dépréciation mise à jour pour le service Change Record	Note de dépréciation mise à jour pour le service Change Record avec des solutions alternatives.	11 septembre 2025
Contrôles Trusted Advisor de sécurité mis à jour pris en charge par Trusted Remediator	Mise à jour des paramètres et contraintes préconfigurés pris en charge pour vérifier Hs4Ma3G108 - les sentiers CloudTrail doivent être intégrés à Amazon Logs CloudWatch	5 septembre 2025
Contrôles Trusted Advisor de sécurité mis à jour pris en charge par Trusted Remediator	Contrôle Trusted Advisor de sécurité mis à jour pour ajouter la version 2 de Hs4Ma3G184 - La journalisation des équilibreurs de charge d'application et des équilibreurs de charge classiques doit être activée	5 septembre 2025
Contrôles d'excellence Trusted Advisor opérationnelle mis à jour pris en charge par la section Trusted Remediator	Mise à jour des contrôles d'excellence Trusted Advisor opérationnelle pris en charge par Trusted Remediator pour ajouter un nouveau contrôle compatible c1fd6b96l4 activé pour les journaux d'accès Amazon S3.	28 août 2025
La section Trusted Remediator a été mise à jour pour inclure du nouveau contenu pour Compute Optimizer	La section Trusted Remediator a été mise à jour pour inclure du nouveau contenu pour les AWS Compute Optimizer recommandations prises en charge.	18 août 2025

Lien vers le glossaire de la table des matières supprimé	AWS Glossaire.	8 août 2025
Lien vers le glossaire de la table des matières supprimé	AWS Glossaire.	8 août 2025
Nouveau champ dans le rapport Patch Daily	Tags d'instance : balises associées à l'ID d' EC2 instance Amazon.	8 août 2025
Nouvelles vérifications de Trusted Remediator	Trusted Advisor contrôles d'optimisation des coûts pris en charge par les contrôles de Trusted Advisor sécurité de Trusted Remediator pris en charge par Trusted Remediator AWSManagedServices-TerminateEC Hs4Ma3G120—2InstanceStoppedForPeriodOfTime, Hs4Ma3G230—2 et c18d2gz150—2. AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV AWSManagedServices-TerminateEC InstanceStoppedForPeriodOfTime	8 août 2025
Mise à jour de la norme IAM au point 3.2	Clarification du langage et suppression de la mention du balisage.	25 juillet 2025
Profils de configuration de Resource Tagger mis à jour dans Accelerate	Ajout d'un nouveau AvailabilityZone filtre dans les profils de configuration de Resource Tagger dans Accelerate.	25 juillet 2025

Rapports d'incidents, demandes de service et questions de facturation mis à jour dans Accelerate.	Les références aux niveaux de service Plus et Premium ont été remplacées par un lien vers le SLA du service.	25 juillet 2025
Gestion des incidents mise à jour dans Accelerate.	Informations mises à jour sur les centres d'opérations.	25 juillet 2025
Page de modèles AMS mise à jour avec les liens corrects.	Correction des liens SLA et SLO.	25 juillet 2025
Mise à jour des options de désactivation des alertes	L'ajout d'un tag vous permet de vous désinscrire de deux alertes supplémentaires.	25 juillet 2025
Nouvelle fonctionnalité pour les sauvegardes	Personnalisez les notifications sur les coffres-forts de sauvegarde à l'aide d'une nouvelle balise.	25 juillet 2025
Section mise à jour pour les configurations prises en charge dans Accelerate	Configurations prises en charge mises à jour pour les systèmes d'exploitation pris en charge et les systèmes d'exploitation supportés en fin de support (EOS) dans Accelerate.	26 juin 2025
Page supprimée Gestion des balises pour la gestion des correctifs dans Accelerate	Page supprimée Gestion des balises pour la gestion des correctifs dans Accelerate car cette fonctionnalité est obsolète.	19 juin 2025

Note de sécurité importante concernant la gestion des correctifs pour les référentiels de correctifs alternatifs.	Note de sécurité importante et bonnes pratiques relatives à l'utilisation de référentiels de correctifs alternatifs dans AMS Accelerate.	10 juin 2025
AMS Accelerate la dépréciation des dossiers de modification.	Le service AMS Accelerate Change Record est obsolète à compter du 1er juillet 2025.	27 mai 2025
Mises à jour des systèmes d'exploitation pris en charge	Les systèmes d'exploitation pris en charge par AMS Accelerate sont mis à jour, certains ajoutés, d'autres supprimés.	22 mai 2025
Remarque concernant les services pris en charge dans la région du Moyen-Orient (EAU).	Support limité pour certains services dans la région du Moyen-Orient (EAU).	22 mai 2025
Uniquement en interne. APIs	Uniquement internes APIs qui apparaissent dans certains CloudWatch journaux.	22 mai 2025
Ajout d'emplacements de journal manquants.	Certains emplacements de journal Windows manquants ont été ajoutés.	22 mai 2025
Mises à jour d'AMS Accelerate Trusted Remediator	Comment utiliser un nouveau paramètre pour personnaliser `preconfigured-parameters` les Trusted Advisor contrôles dans Trusted Remediator.	22 mai 2025

FAQ et mises à jour d'AMS Accelerate Trusted Remediator.	Plusieurs mises à jour Trusted Advisor des contrôles pris en charge, FAQ sur Trusted Remediator (ajout de la section « Quelles ressources Trusted Remediator déploie-t-il sur vos comptes ? ») , et bien plus encore. Voir également les Trusted Advisor contrôles pris en charge par Trusted Remediator.	8 mai 2025
Mise à jour des contrôles de sécurité AMS Accelerate Standard.	Ajout de contrôles « Partage de groupes de sécurité ».	8 mai 2025
Accélérez la mise à jour des alertes de surveillance	Des alertes supplémentaires ont été ajoutées, plus le nom de l'alerte a été ajouté à la colonne Notes.	28 avril 2025
Accélérez l'inventaire des ressources.	Le fichier de feuille de calcul de l'inventaire des ressources (compressé) est mis à jour.	24 avril 2025
Accélérez la localisation des journaux.	Des emplacements de journal supplémentaires ont été ajoutés.	24 avril 2025
Accélérez les nouveaux rôles et responsabilités (RACI) pour la réponse aux incidents de sécurité.	RACI pour la réponse aux incidents de sécurité.	27 mars 2025

Accélérez la nouvelle alerte de correction automatique Amazon RDS.	ID d'alerte : - 0224, se déclenche lorsque le stockage alloué demandé atteint ou dépasse le seuil de stockage maximal configuré.	27 mars 2025
Accélérez la mise à jour du modèle de rôle d'intégration.	Le modèle de rôle d'intégration AMS Accelerate a été mis à jour pour prendre en charge GovCloud les régions AWS.	25 mars 2025
Accélérez la nouvelle alerte RDS de remédiation automatique.	RDS-EVENT-0224 ajouté.	17 mars 2025
Accélérer une nouvelle fonctionnalité : les notifications d'incidents.	Vous pouvez l'utiliser AppRegistry pour créer des applications et personnaliser les notifications d'incident pour ces applications.	13 mars 2025
Accélérez la mise à jour du seuil de surveillance des alarmes RDS.	Le seuil d'alarme d'utilisation moyenne du processeur RDS a été modifié de 75 % à 90 %.	20 février 2025
Accélérez la mise à jour vers le tableau de correction automatique des alertes AMS.	Le tableau de correction des alertes a été enrichi de nouveau contenu.	20 février 2025
Accélérer la nouvelle fonctionnalité : conserver les alarmes.	Vous pouvez configurer Alarm Manager pour conserver les alarmes au CloudWatch lieu de les supprimer automatiquement.	20 février 2025

Rapports en libre-service mis à jour avec de nouvelles options de données pour l'affichage des rapports agrégés	Des options de données ont été ajoutées pour inclure les nouveaux nom de champ :`Admin Account ID`, nom de champ du jeu de données : `aws_admin_account_id` et définition : `Trusted AWS Organization account enabled by the customer` pour les rapports en libre-service suivants : • Rapport de patch (quotidien) • Rapport de sauvegarde (quotidien) • Rapport d'incident (hebdomadaire) • Tableau de bord Resource Tagger • Tableau de bord des règles de configuration de sécurité	28 janvier 2025

Ajout de AWS Trusted Advisor vérifications supplémentaires prises en charge par Trusted Remediator	Les Trusted Advisor vérifications suivantes sont désormais prises en charge par Trusted Remediator :
	• Optimisation des coûts
	  • c1cj39rr6v - Configuration incomplète de l'interruption du téléchargement en plusieurs parties sur Amazon S3
	• Sécurité
	  • Hs4Ma3G199 - Les instances de base de données RDS doivent publier des journaux dans Logs CloudWatch
	  • Hs4Ma3G326 - Le paramètre de blocage de l'accès public à Amazon EMR doit être activé
	  • Hs4Ma3G272 - Les utilisateurs ne doivent pas avoir d'accès root aux instances de bloc-notes AI SageMaker
	  • Hs4Ma3G325 - La journalisation des audits doit être activée sur les clusters EKS
	  • HHs4Ma3G118 - Les groupes de sécurité VPC par défaut ne doivent pas autoriser le trafic entrant ou sortant
		28 janvier 2025

    - Hs4Ma3G127 - API Gateway REST et la journalisation de l'exécution de l'API WebSocket doivent être activées
    - Hs4Ma3G124 - Les instances EC2 Amazon doivent utiliser le service de métadonnées d'instance version 2 () IMDSv2
- Tolérance aux pannes
    - c1qf5bt013 - Le dimensionnement automatique du stockage est désactivé pour les instances de base de données Amazon RDS
    - 7q GXs KIUw - Vidange de la connexion Classic Load Balancer
    - c18d2gz106 - Amazon EBS n'est pas inclus dans le forfait AWS Backup
    - c18d2gz107 - La table Amazon DynamoDB n'est pas incluse dans le forfait AWS Backup
    - cc18d2gz117 - Amazon EFS n'est pas inclus dans le forfait AWS Backup
    - c18d2gz105 - Équilibrage de charge croisée du Network Load Balancer

- c1qf5bt026 - Le paramètre synchronous_commit d'Amazon RDS est désactivé
- c1qf5bt030 - Le paramètre innodb_flush_log_at_trx_commit d'Amazon RDS n'est pas 1
- c1qf5bt031 - Le paramètre sync_binlog d'Amazon RDS est désactivé
- c1qf5bt036 - Le réglage du paramètre innodb_default_row_format d'Amazon RDS n'est pas sûr
- c18d2gz144 - La surveillance détaillée d'Amazon n'est pas activée EC2

- Excellence opérationnelle
  - c18d2gz125 - Amazon API Gateway n'enregistre pas les journaux d'exécution
  - c18d2gz168 - La protection de charge élastique n'est pas activée pour les équilibreurs de charge BalancingDeletion
  - c1qf5bt012 - Amazon RDS Performance Insights est désactivé

	• Performances
	  • c1qf5bt021 - Paramètre Amazon RDS innodb_change_buffering utilisant une valeur inférieure à la valeur optimale
	  • c1qf5bt025 - Le paramètre Autovacuum d'Amazon RDS est désactivé
	  • c1qf5bt028 - Le paramètre enable_indexonlyscan d'Amazon RDS est désactivé
	  • c1qf5bt029 - Le paramètre enable_indexscan d'Amazon RDS est désactivé
	  • c1qf5bt032 - Le paramètre innodb_stats_persistent d'Amazon RDS est désactivé
	  • c1qf5bt037 - Le paramètre Amazon _logging est activé RDSgeneral	

Feuille de calcul de l'inventaire des ressources mise à jour	Feuille de calcul de l'inventaire des ressources mise à jour.	23 janvier 2025
Nouvelle fonctionnalité AMS : rapports agrégés en libre-service	Les rapports agrégés en libre-service (SSR) vous fournissent une vue des rapports en libre-service existants agrégés au niveau de l'organisation, entre comptes.	21 janvier 2025

Nouvelle fonctionnalité d'accélération des correctifs : Patch Hooks	Utilisez cette fonctionnalité pour configurer des « hooks » avec des documents de commande SSM afin d'exécuter des commandes au niveau du système d'exploit ation avant ou après l'applica tion de correctifs.	16 janvier 2025
Mise à jour de la section Fonctionnement de la surveilla nce	Ajout d'informations sur une nouvelle fonctionnalité, en configurant les notifications d'alerte par ressource ou par ID d'instance, plutôt que par incident.	8 janvier 2025
Mise à jour de la section d'intégration d'EKS Monitoring and Incidents Management	Mise à jour de la note relative à la procédure d'intégration afin de préciser à quel moment les signaux d'alerte sont suspendus et repris.	19 décembre 2024
Journal du compte membre ajouté à Trusted Remediator	Vous pouvez utiliser le journal des comptes des membres pour trouver l'identifiant du compte, l'enregistrement et Régions AWS l'heure d'exécution de chaque compte membre.	19 décembre 2024
Conditions préalables à l'utilisa tion de l'agent SSM	Le contenu relatif au blocage du trafic sortant est mis à jour.	4 décembre 2024

L'accélération de la surveillance et de la gestion des incidents pour EKS est désormais prise en charge dans la région Asie-Pacifique (Hong Kong) Région AWS	L'Asie-Pacifique (Hong Kong) est désormais pris en charge par Accelerate Monitoring and Incident Management for EKS	21 novembre 2024
Tableau des offres Operations On Demand mis à jour	Les systèmes d'exploitation suivants sont pris en charge pour les mises à niveau sur place : • Microsoft Windows 2016 à Microsoft Windows 2022 et versions ultérieures	11 novembre 2024
Accelerate Monitoring and Incidents Management for EKS est désormais pris en charge en Afrique (Cape Town) Région AWS.	L'Afrique (Le Cap) est désormais soutenue par Accelerate Monitoring and Incident Management for EKS	4 novembre 2024

Tableau des offres Operations On Demand mis à jour	Les systèmes d'exploitation suivants sont pris en charge pour les mises à niveau sur place : • Microsoft Windows 2012 R2 vers Microsoft Windows 2016 et versions ultérieures • Red Hat Enterprise Linux 7 vers Red Hat Enterprise Linux 8 • Red Hat Enterprise Linux 8 vers Red Hat Enterprise Linux 9 • Oracle Linux 7 vers Oracle Linux 8	1er novembre 2024
Modèle de démarrage rapide mis à jour	Schéma, paramètres du modèle et fichier modèle yaml mis à jour.	28 octobre 2024

Trusted Advisor chèques ajoutés à Trusted Remediator dans AMS	Les Trusted Advisor vérifications suivantes sont désormais disponibles dans Trusted Remediator : • Z4 AUBRNSmz - Adresses IP élastiques non associées • c18d2gz128 - Référentiel Amazon ECR configuré sans politique de cycle de vie • c18d2gz138 - Restauration DynamoDB Point-in-time • Hs4Ma3G323 - Dynamo DBtables devrait avoir la protection contre la suppression activée • Hs4Ma3G247 - Amazon Transit EC2 Gateway ne doit pas accepter automatiquement les demandes de pièces jointes VPC • Hs4Ma3G308 - La protection contre la suppression des clusters Amazon DocumentDB doit être activée • Hs4Ma3G299 - La protection contre la suppression des clusters de base de données Neptune doit être activée • Hs4Ma3G306 - Les instantanés de cluster manuels Amazon	25 octobre 2024

	DocumentDB ne doivent pas être publics • Hs4Ma3G109 - la validation du fichier CloudTrail journal doit être activée • Hs4Ma3G217 - les environnements de CodeBuild projet doivent disposer d'une journalisation AWS Configuration4 • Hs4Ma3G158 - Les documents SSM ne doivent pas être publics • Hs4Ma3G319 - La protectio n contre les suppressions doit être activée sur les pare-feux Network Firewall	
Configurations compatibles mises à jour	Mise à jour des systèmes d'exploitation Oracle Linux pris en charge vers les versions 9.0-9.3, 8.0-8.9, 7.5-7.9.	24 octobre 2024
Nouvelle section ajoutée à Offboard depuis AMS Accelerate	Instructions sur la procédure de déconnexion avec les dépendances d'Alarm Manager et de Resource Tagger ajoutées à Offboard depuis AMS Accelerate.	24 octobre 2024
Le tableau de bord Resource Tagger est désormais disponible.	Le tableau de bord Resource Tagger est désormais disponible dans les rapports en libre-service.	26 septembre 2024

Vous pouvez désormais inclure plusieurs adresses e-mail dans les alertes basées sur des balises.	Les adresses e-mail multiples sont désormais prises en charge dans les alertes basées sur des balises.	20 septembre 2024
Les limites d'AMS Accelerate sont désormais incluses dans la gestion des correctifs AMS.	Les limites d'AMS Accelerate sont incluses dans la gestion des correctifs : créez une fenêtre de maintenance des correctifs.	30 août 2024
Mise à jour AMS Accelerate Account Discovery	Une nouvelle section dans Account Discovery a été ajoutée pour Amazon EC2 Instance Evaluation.	29 août 2024
La ligne de base de correctifs par défaut d'AMS Accelerate est désormais disponible pour les systèmes d'exploitation Ubuntu.	La ligne de base de correctifs par défaut d'AMS Accelerate est désormais disponible pour les systèmes d'exploitation Ubuntu.	22 août 2024
Mise à jour AMS Accelerate Account Discovery	Quatre nouveaux appels AWS d'API ont été ajoutés à la section AWS CloudTrai l Évaluation du tableau de contrôle opérationnel.	2 août 2024
Trusted Remediator prend désormais en charge une vérification supplémentaire	Trusted Remediator prend désormais en charge le contrôle de sécurité Hs4Ma3G192. Les instances de base de données RDS devraient interdire l'accès public.	30 juillet 2024

AMS prend désormais en charge le pare-feu DNS Amazon Route 53 Resolver	AMS prend désormais en charge le pare-feu DNS Amazon Route 53 Resolver	30 juillet 2024
AMS Accelerate onboarding_role_minimal.zip contient désormais du code Terraform	AMS Accelerate onboarding_role_minimal.zip contient désormais du code Terraform.	30 juillet 2024
Tableau de bord des règles de configuration de sécurité	Le tableau de bord des règles de configuration de sécurité est désormais disponible dans les rapports en libre-service.	24 juillet 2024
AMS Accelerate prend désormais en charge Oracle Linux 8.9, RHEL 8.10 et RHEL 9.4.	AMS Accelerate prend désormais en charge Oracle Linux 8.9, RHEL 8.10 et RHEL 9.4.	5 juillet 2024
Mise à jour du processus de découverte des comptes AMS Accelerate.	Le processus de découverte du compte utilisé lors de l'intégration Comptes AWS à AMS Accelerate est mis à jour.	1 juillet 2024
Trusted Remediator est désormais disponible.	Trusted Remediator, une solution AWS Managed Services qui automatise la correction des AWS Trusted Advisor contrôles, est désormais disponible.	24 juin 2024
Événements du pare-feu DNS Amazon Route 53 Resolver dans Security Incident Response.	AMS surveille désormais les événements du pare-feu DNS d'Amazon Route 53 Resolver dans Security Incident Response	21 juin 2024

Systèmes d'exploitation pris en charge mis à jour	AMS Accelerate prend désormais en charge les AlmaLinux versions 8.3-8.9, 9.0-9.2 (uniquement AlmaLinux compatible avec l'architecture x86)	19 juin 2024
La limite automatique du profil d'instance augmente désormais si la valeur par défaut est respectée.	AMS augmente désormais la limite de profil d'instance par défaut à 20 si la limite par défaut de 10 est atteinte.	18 juin 2024
La fonctionnalité d'installation automatique de l'agent AMS SSM est désormais activée par défaut.	La fonctionnalité d'installation automatique de l'agent AMS SSM est activée par défaut pour les comptes intégrés après le 6 mars 2024.	7 juin 2024
FAQ sur la sécurité ajoutée à la gestion de la sécurité.	Une FAQ sur la sécurité est désormais disponible. Elle couvre les questions courantes concernant les meilleures pratiques de sécurité, les contrôles, les modèles d'accès et les mécanismes d'audit utilisés lorsqu'un ingénieur des opérations ou un automate AMS accède à vos comptes.	3 juin 2024
Des AWS régions supplémentaires sont désormais prises en charge par la surveillance et la gestion des incidents pour Amazon EKS.	Trois AWS régions supplémentaires sont désormais prises en charge par la surveillance et la gestion des incidents pour Amazon EKS.	23 mai 2024

Les notifications de demande de service sont désormais envoyées avant les fenêtres de maintenance des correctifs.	L'application de correctifs AMS Accelerate crée une nouvelle demande de service 4 jours avant la période de maintenance des correctifs. Vous pouvez utiliser la demande de service pour communiquer avec AMS pour modifier le correctif ou pour ignorer un correctif.	3 mai 2024
Seuils d'alerte ajoutés au tableau des alertes de base de surveillance AMS Accelerate EKS.	Les seuils d'alerte détaillés sont désormais disponibles dans le tableau des alertes de base pour la surveillance Amazon EKS.	3 mai 2024
Mise à jour : profils de configuration d'Alarm Manager.	Ajout de remarques sur la création d'alarmes de détection d'anomalies avec Alarm Manager.	25 avril 2024
Ajouts aux profils de configuration de Resource Tagger.	Les tables DynamoDB et les compartiments Amazon S3 sont désormais disponibles dans Resource Tagger	25 avril 2024
Ajout d'une section d'informations sur la gestion des événements planifiés (PEM).	Des informations détaillées sur l'offre de services PEM sont désormais disponibles dans le guide de l'utilisateur d'AMS Accelerate.	25 avril 2024
AMS prend en charge Red Hat Enterprise Linux (RHEL) 9.x.	AMS prend en charge Red Hat Enterprise Linux (RHEL) 9.x.	25 avril 2024

AMS Accelerate prend en charge le reporting pour toutes les configurations AWS régionales.	AMS Accelerate prend en charge les rapports d'inventaire SSM pour toutes les configurations AWS régionales.	25 avril 2024
Mise à jour : politiques AWS gérées.	Mise à jour du AWSManagedServicesDeploymentToolkitPolicy avec les nouvelles autorisations ECR.	4 avril 2024
Mise à jour : section Profils de configuration du Resource Tagger	Ajouté `AWS::EFS::FileSystem` à la ResourceTypeliste.	21 mars 2024
Mise à jour : rapports d'incidents et demandes de service dans la section Accélérer.	Le titre du sujet a été modifié pour devenir Rapports d'incidents, demandes de service et questions de facturation dans Accelerate. Ajout d'une nouvelle section, Questions relatives à la facturation.	21 mars 2024
Mise à jour : section Fonctionnement de la gestion des demandes de service.	Ajout de précisions sur la manière dont AMS gère les demandes de service contenant une demande de fonctionnalité ou un bogue.	21 mars 2024
Mise à jour : création du rôle aws_managedservices_onboarding_role avec une section AWS CloudFormation	Commandes ajoutées à partir desquelles créer le rôle AWS CloudShell.	21 mars 2024
Mise à jour : modèle de démarrage rapide (facultatif)	Des commandes ont été ajoutées pour télécharger le modèle AWS CloudShell.	21 mars 2024

Nouveaux types de ressources disponibles pour les profils de configuration d'Alarm Manager.	Des types de ressources pour Amazon FSx, Amazon EFS et Elasticsearch ont été ajoutés aux profils de configuration d'Alarm Manager.	21 mars 2024
Des substitutions de pseudoparamètres supplémentaires sont disponibles pour le profil de configuration.	Ajout des substitutions de FSx pseudoparamètres Amazon EFS et Amazon.	21 mars 2024
Ajout d'une nouvelle section aux fonctionnalités dans la rubrique Description du service.	Ajout d'une nouvelle section, Gestion des demandes de service dans le cadre des fonctionnalités d'AMS Accelerate.	21 mars 2024
Nouvelles colonnes ajoutées au rapport en libre-service Rapport d'incident hebdomadaire	De nouvelles colonnes ont été ajoutées au rapport hebdomadaire sur les incidents afin que vous puissiez filtrer les incidents en fonction du trimestre, du mois, de la semaine ou du jour où l'incident a été créé ou résolu.	11 mars 2024

Mises à jour antérieures

Le tableau suivant décrit les modifications importantes apportées à la documentation du guide AMS Accelerate avant mars 2024.

Modification	Description	Date
Améliorations apportées à l'intégration des CloudTrail sentiers avec AMS Accelerate	Améliorations apportées à l'intégration des CloudTrail sentiers AMS Accelerate :	23 février 2024

Modification	Description	Date
	• Collectez toutes les politiques relatives aux compartiments en un seul bloc • Supprimer le deuxième ID d' AWS organisat ion dans les déclarations de politique • Clarifier les exigences de l'environnement client Pour de plus amples informations, veuillez consulter Passez en revue et mettez à jour vos configurations pour permettre à AMS Accelerat e d'utiliser votre CloudTrail parcours.	
Mise à jour : processus d'intégration du compte.	Restructuration de la section relative au processus d'enregistrement du compte afin de clarifier les étapes. Ajout également d'un modèle de démarrage rapide en option pour les fonctionnalités d'intégration. Consultez (Facultatif) Modèle de démarrage rapide dans Accelerate.	22 février 2024
Mise à jour : Déchargement d'AMS Accelerate.	Mise à jour de la section des considérations relatives à l'offboarding d'AMS Accelerate pour indiquer que le `ams-access-management` CloudFormation stack et le rôle `ams-acces s-management` IAM ne sont pas supprimés par le processus de déchargement. Consultez Effets d'offboarding AMS Accelerate.	22 février 2024
Mise à jour : conformité de la configuration dans Accelerate.	Le terme « Rapport d'incident » a été remplacé par « Demande de service », le cas échéant, afin d'éviter toute confusion quant à ces termes. Consultez Conformité des configurations dans Accelerate.	22 février 2024

Modification	Description	Date
Mise à jour : découverte de comptes dans Accelerate.	Découverte des comptes réorganisée dans Accelerate afin de mieux regrouper les prérequis dans la section correspondante. Consultez Étape 1. Découverte de comptes dans Accelerate.	22 février 2024
Renommé : le patch AMS rapporte à la gestion des hôtes AMS.	Le reporting AMS Patch a été renommé AMS host management et le rapport, Patch Details, a été renommé en rapport SSM Agent Coverage. Consultez Rapports de gestion des hôtes AMS.	22 février 2024
Catalogue des opérations à la demande mis à jour	Mise à jour du tableau des offres Operations on Demand afin de supprimer les référence s à la « santé » dans`Amazon EKS cluster maintenance` . Consultez Demande d'opérations AMS à la demande.	22 février 2024
Routeur d'événements AMS mis à jour	Mise à jour `AMSCoreRule` de la section AMS Event Router. Consultez Utilisation des règles EventBridge gérées par Amazon dans AMS.	22 février 2024
Systèmes d'exploitation pris en charge mis à jour.	Systèmes d'exploitation pris en charge mis à jour pour inclure SUSE Linux Enterprise Server 15 SP5. Consultez Configurations prises en charge.	22 février 2024

Modification	Description	Date
Automatisation actualisée EC2 de la correction de l'utilisation des volumes	Mise à jour de la section d'automatisation de la correction de l'utilisation des EC2 volumes avec un calendrier d'extension de capacité correct. Consultez EC2 automatisation de la correction de l'utilisation des volumes.	22 février 2024
Mise à jour : passez en revue et mettez à jour vos configurations pour permettre à Accelerate d'utiliser votre CloudTrail parcours	Mise à jour de la section relative à la politique du bucket CloudTrail S3 d'AMS Accelerate Organization. Consultez Passez en revue et mettez à jour vos configurations pour permettre à AMS Accelerate d'utiliser votre CloudTrail parcours.	15 février 2024
Nouvelle fonctionnalité ajoutée : installation automatique de l'agent SSM	Ajout d'une nouvelle section pour l'installation automatique de l'agent SSM Consultez Installation automatique de l'agent SSM.	26 janvier 2024
Mise à jour : configurations prises en charge	Informations supplémentaires concernant les versions prises en charge de AWS Control Tower Consultez Configurations prises en charge.	26 janvier 2024
Mise à jour : rapports sur les correctifs AMS.	Trois sections ont été supprimées des rapports sur les correctifs AMS : • Rapport récapitulatif des détails de l'instance de correctif • Rapport sur les détails des correctifs • Instances signalées pour lesquelles des correctifs ont été manqués Consultez Rapports de gestion des hôtes AMS.	22 décembre 2023

Modification	Description	Date
Mise à jour : accélérez les prérequis d'intégration.	Mise à jour des plans de support requis pour intégrer AMS Accelerate. Consultez Accélérez les prérequis d'intégration.	15 décembre 2023
Mise à jour : créez une fenêtre de maintenance des correctifs.	La section du cycle de correctifs par défaut a été supprimée car cette fonctionnalité est obsolète. Consultez Création d'une fenêtre de maintenance des correctifs dans AMS.	13 décembre 2023
Mise à jour : paramètres de notification dans Accelerate.	Clarification de l'adresse e-mail utilisée pour les notifications. Pour plus d'informations, consultez Paramètres de notification dans Accelerate.	12 décembre 2023
Mise à jour : `AMSAccelerateCustomerAccessPolicies` modèle.	Le `AMSAccelerateCustomerAccessPolicies` modèle a été mis à jour pour corriger une erreur de syntaxe. Pour plus d'informations, consultez Autorisations d'utilisation des fonctionnalités AMS.	12 décembre 2023
Ajouté : révisions de sécurité des demandes de modification	Ajout d'une nouvelle section Révisions de sécurité des demandes de modification sous Gestion de la sécurité. Pour plus d'informations, consultez Examens de sécurité des demandes de modification.	11 décembre 2023
Mise à jour : resource_inventory.xlsx	Le fichier resource_inventory.xlsx a été mis à jour pour inclure les rôles d'analyste de sécurité. Pour plus d'informations, consultez Inventaire des ressources pour Accelerate.	17 novembre 2023

Modification	Description	Date
Mise à jour : description du ams-access-admin-operations rôle	ams-access-admin-operationsDescription mise à jour. Pour plus d'informations, consultez Pourquoi et quand AMS accède à votre compte et Authentification avec des identités dans AMS Accelerate.	17 novembre 2023
Mise à jour : considérations relatives à l'offboarding avec AMS Accelerate	Section de sécurité mise à jour pour clarifier ce qui est disponible sur Amazon GuardDuty et AWS Config les règles après le déchargement. Pour plus d'informations, consultez Effets d'offboarding AMS Accelerate.	17 novembre 2023
Ajouté : surveillance et gestion des incidents pour Amazon EKS	La surveillance et la gestion des incidents pour Amazon EKS surveillent vos ressources Amazon EKS pour détecter les défaillances, la dégradation des performances et les problèmes de sécurité. Pour plus d'informations, consultez Surveillance et gestion des incidents pour Amazon EKS dans AMS Accelerate.	14 novembre 2023
Mise à jour : balisage	Ajout d'informations sur le balisage fourni par le client. Pour plus d'informations, consultez Tags fournis par le client dans Accelerate.	7 novembre 2023

Modification	Description	Date
Mise à jour : profils de configuration de Resource Tagger	Ajouté AWS::AutoScaling::AutoScalingGroup, AWS::EKS::Cluster, AWS::Elasticsearch ::Domain, and AWS::FSx::FileSystem à la section Filtre. Pour plus d'informations, consultez Profils de configuration de Resource Tagger dans AMS Accelerate.	27 octobre 2023
Mise à jour : Description du service	Ubuntu 22.04 a été ajouté aux systèmes d'exploitation pris en charge. Consultez Service description (Description du service).	29 septembre 2023
Mise à jour : conditions préalables à l'intégration d'AMS Accelerate	Ajout d'une note aux points de terminaison VPC AMS Accelerate pour inclure un modèle. CloudFormation Consultez Accélérez les prérequis d'intégration.	29 septembre 2023
Mise à jour : Detect	Type de protection des terminaux supprimé de la réponse de sécurité AMS Accelerate. Consultez Détection.	29 septembre 2023
Mise à jour : alertes issues de la surveillance de base dans AMS	Ajouté AWS Outposts au tableau des alertes issues de la surveillance de base. Consultez Détection monitoring-default-metrics.	29 septembre 2023
Mise à jour : créez le rôle aws_managedservice s_onboarding_role avec AWS CloudFormation	Capture d'écran mise à jour pour Spécifier les détails de la pile Consultez Créez `aws_managedservices_onboarding_role` avec AWS CloudFormation for Accelerate.	29 septembre 2023

Modification	Description	Date
Mise à jour : Amazon EventBridge Managed Rules déployée par AMS Accelerate	Ajout d'une nouvelle AMSCorerègle EventBridge gérée par AMS Accelerate Amazon. Mise à jour de la règle EventBridge gérée par AMS Accelerate Amazon AMSAccess RolesRulepour ajouter un nouveau rôle. Pour plus d'informations, consultez Amazon EventBridge Managed Rules déployées par AMS .	19 septembre 2023
Mise à jour : profils de configuration d'Alarm Manager	Ajout d'identifiants de substitution de pseudoparamètres d'AWS Outposts. Consultez Surveillance et gestion des événements dans AMS Accelerate.	11 septembre 2023
Mise à jour : profils de configuration de Resource Tagger	Le type de ressource AWS Outposts a été ajouté. Consultez Accélérer le profil de configuration : substitution de pseudoparamètres.	11 septembre 2023
Mise à jour : Services pris en charge	Amazon Elastic File System a été ajouté à la section Services surveillés par CloudWatch des alarmes. Pour plus d'informations, consultez Service description (Description du service).	6 septembre 2023

Modification	Description	Date
Mise à jour : surveillance des correctifs et correction des défaillances	La note suivante a été ajoutée à la section Utilisation de Patch Orchestrator : « Les alertes d'échec des correctifs ne sont pas créées pour les instances dont les systèmes d'exploitation ne sont pas pris en charge ou qui sont arrêtées pendant la période de maintenan ce » Pour plus d'informations, consultez Comprendr e la gestion des correctifs dans AMS Accelerat e.	6 septembre 2023
Mise à jour : manuel de réponse clarifié aux événements malveillants	Manuel de réponse clarifié aux événements malveillants pour la réponse aux incidents de sécurité. Pour plus d'informations, consultez Réponse aux incidents de sécurité dans AMS .	6 septembre 2023
Mise à jour : connexion de votre compte Accelerate à Transit Gateway	Étapes clarifiées pour connecter un nouveau compte Accelerate VPC au réseau AMS Multi-Account Landing Zone (création d'une pièce jointe TGW VPC) : voir Connexion de votre compte Accelerate à Transit Gateway pour plus d'informations.	5 septembre 2023
Mise à jour : alertes issues de la surveillance de base dans AMS	Suppression de la référence à deux alarmes AMSRead LatencyAlarm obsolètes et. AMSWrite LatencyAlarm Pour plus d'informa tions, consultez Alertes issues de la surveilla nce de base dans AMS.	5 septembre 2023
Ajouté : AMS Event Router	Ajout de la documentation pour AMS Event Router. Voir Utilisation des règles EventBrid ge gérées par Amazon dans AMS pour plus d'informations.	5 septembre 2023

Modification	Description	Date
Mise à jour : liste des pseudoparamètres d'Alarm Manager.	Mise à jour de la liste des pseudoparamètres d'Alarm Manager. EC2 le paramètre de nom d'instance a été ajouté aux configurations d'alarme d' EC2 instance et de EC2 disque. Pour plus d'informations, consultez Accélérer le profil de configuration : substitution de pseudoparamètres.	29 août 2023
Ajouté : AMS Access Offboarding	Une considération supplémentaire a été prise en compte lors de la désintégration d'AMS Access. Consultez Effets d'offboarding AMS Accelerate.	24 août 2023
Ajouté : AMS Security Incident Response	Ajout de documentation sur l'utilisation d'AMS Security Incident Response. Consultez Réponse aux incidents de sécurité dans AMS .	18 août 2023
Mise à jour : rôles d'accès AMS Accelerate	Correction d'une faute de frappe dans les noms de rôles. Consultez AWS Identity and Access Management dans AMS Accelerate.	10 août 2023
Mise à jour : déclarations de politique	Les noms de rôles codés en dur ont été remplacés par des caractères génériques. Consultez Passez en revue et mettez à jour vos configurations pour permettre à AMS Accelerate d'utiliser votre CloudTrail parcours.	10 août 2023
Mise à jour : liste des services surveillés avec alertes EFS.	Mise à jour de la liste des services de surveillance avec de nouvelles alertes EFS pour la surveillance de base AMS. 4 nouveaux types d'alertes EFS ont été ajoutés. Pour plus d'informations, consultez Alertes issues de la surveillance de base dans AMS.	3 août 2023

Modification	Description	Date
Mise à jour : tableau d'inventaire des ressources accéléré	ams-backup-config-rule-stack et les ressources associées ont été supprimés. Consultez Inventaire des ressources pour Accelerate.	18 juillet 2023
Mise à jour : rôles d'accès AMS Accelerate	<8-digit hash>Les rôles ams-backup-config-rule -st- amsBackupAlert ConfigRule - <8-digit hash>et ams-backup-config-rule -st-amsBackupPlan ConfigRule H- ont été supprimés. Consultez AWS Identity and Access Management dans AMS Accelerate.	18 juillet 2023
Mise à jour : liste des alertes RDS surveillées.	Mise à jour de la liste des alertes RDS pour la surveillance de base AMS. 9 nouveaux types d'alertes RDS ont été ajoutés et 3 types d'alertes RDS existants ont été supprimés. Pour plus d'informations, consultez Alertes issues de la surveillance de base dans AMS.	19 juin 2023
Nouveau : rôles d'accès AMS Accelerate	Ajout de nouveaux rôles d'accès pour AMS Security.	16 juin 2023
Nouveau : la gestion des CloudTrail journaux AMS Accelerate peut désormais utiliser les CloudTrail traces des clients.	Options mises à jour prises en charge par Accelerate pour la gestion des CloudTrail journaux, notamment le suivi accéléré du déploiement ou l'intégration avec le CloudTrail compte géré par le client ou le suivi de l'organisation. Pour plus d'informations, consultez Passez en revue et mettez à jour vos configurations pour permettre à AMS Accelerate d'utiliser votre CloudTrail parcours.	9 juin 2023

Modification	Description	Date
Mise à jour : rapport de configuration des réponses aux règles AMS Accelerate Config.	Rapports mis à jour sur demande pour le rapport de AWS configuration de Config Rules Response. Voir Accélérer les mises à jour des rapports sur demande. Consultez Rapport de configuration des réponses aux règles de configuration AMS Config.	26 mai 2023
Mise à jour : Politique de date de début de facturation du service.	Définitions mises à jour de la date de début de facturation dansTermes clés d'AMS.	15 mai 2023
Mise à jour : politiques AWS gérées.	J'ai mis à jour le AWSManaged ServicesD eploymentToolkitPolicy avec de nouvelles autorisations CFN et ECR, et a défini les actions existantes à l'aide de caractères génériques. Voir Accélérer les mises à jour des rôles liés à un service. Consultez Accélérez les mises à jour des rôles liés aux services.	9 mai 2023
Mise à jour : accès aux liens relatifs aux politiques relatives aux rôles.	Les rôles d'accès peuvent désormais être téléchargés directement depuis les emplacements des compartiments Accelerate S3. Consultez Pourquoi et quand AMS accède à votre compte et AWS Identity and Access Management dans AMS Accelerate.	
Mise à jour : rapport mensuel en libre-service sur la facturation.	Remarque ajoutée : les rapports de facturation mensuels ne sont disponibles que sur un compte Management Payer (zone de destination multi-comptes AMS Advanced), mais sont disponibles pour tous les comptes gérés par AMS Accelerate associés. Consultez Rapport de facturation (mensuel).	13 avril 2023

Modification	Description	Date
Mise à jour : liste des alertes.	CloudTrail Références supprimées. Consultez Gestion des journaux dans AMS Accelerate.	13 avril 2023
Mise à jour : liste des alertes.	Ajout de trois nouvelles alertes relatives à l'agent SSM. Consultez Alertes issues de la surveillance de base dans AMS.	13 avril 2023
Mise à jour : Accélérez les prérequis.	Il a été précisé qu'Accelerate nécessite la mise en place de l'un des quatre plans de support AWS et exclut le plan pour développeurs. Consultez Accélérez les prérequis d'intégration.	13 avril 2023
Mise à jour : accélérer la politique des rôles liés aux services.	Le fichier zip de politique du service Contacts a été mis à jour. Consultez AWS politiques gérées pour AMS Accelerate.	13 avril 2023
Mise à jour : AMS Resource Scheduler.	Nom de rôle incorrect AWSManagedServices-DescribeScheduleOrPeriod, corrigé en AWSManagedServices-DescribeScheduleOrPeriods. Consultez Optimisation des coûts avec AMS Resource Scheduler.	13 avril 2023
Mise à jour : politiques AWS gérées.	Mis à jour Constatations et réponses personnalisées avec des instructions pour mettre à jour les réponses personnalisées dans un ou plusieurs comptes.	13 avril 2023

Modification	Description	Date
Mise à jour : Resource Tagger	Des avertissements ont été ajoutés concernant « la spécification du nom de votre nouvelle configuration (SampleConfigurationBlock dans l'exemple fourni) car vous risquez de remplacer par inadvertance la configuration gérée par AMS par le même nom ». Consultez Cas d'utilisation de Resource Tagger dans AMS Accelerate.	16 mars 2023
Mise à jour : Patch RACI	Plusieurs mises à jour et clarifications du RACI pour les correctifs. Consultez Service description (Description du service).	16 mars 2023
Mise à jour : actions dans le kit de déploiement SLR JSON	Politique et actions mises à jour. Voir : Utilisation de rôles liés à un service pour AMS Accelerate.	16 mars 2023
Mise à jour : correction automatique	Suppression du support LVM pour l'automatisation des EC2 volumes. Voir : Correction automatique des alertes par AMS.	16 mars 2023
Mise à jour : Accélérez l'intégration.	Utilisation clarifiée des rôles, en particulier du rôle minimal. Le modèle pour créer des rôles AMS	16 mars 2023
Mise à jour : rapports en libre-service.	Les rapports de sauvegarde quotidiens prennent désormais en charge les régions principales et secondaires. Les deux sont indiqués dans le champ Région ressource deRapport de sauvegarde (quotidien).	16 mars 2023

Modification	Description	Date
Mise à jour : conseils d'application des correctifs	Ajout d'un avertissement pour ne pas personnaliser les lignes de base d'application de correctifs par défaut, qui sont gérées par AMS. Créez plutôt une nouvelle ligne de base de correctifs personnalisée. Voir : Ligne de base de correctifs par défaut etBase de correctifs personnalisée avec AMS Accelerate.	16 mars 2023
Politique de résiliation du service mise à jour.	Définitions mises à jour de la fin du service et de la date de fin du service dansTermes clés d'AMS. Les avis de résiliation doivent être émis au plus tard le 20 du mois précédant votre dernier mois complet.	16 mars 2023
Mise à jour : politiques AWS gérées.	Nom de la politique clarifié :Rôle lié au service des contacts pour AMS Accelerate.	16 févr. 2023
Nouveau : politiques AWS gérées.	Politique ajoutée :Rôle lié au service des contacts pour AMS Accelerate.	16 févr. 2023
Mise à jour : Conformité de la configuration.	Correction d'un mot mal orthographié dans :. Conformité des configurations dans Accelerate	16 févr. 2023
Nouveau contenu : non pris en charge OSes	Informations supplémentaires sur les services fournis par AMS pour les systèmes d'exploitation non pris en charge (OSes), voirFonctionnalités pour les systèmes d'exploitation non pris en charge dans Accelerate.	16 févr. 2023
Mise à jour : création de fenêtres de correctifs	Ajout d'un lien permettant d' CloudShell utiliserCréez une fenêtre de maintenance avec l'interface de ligne de commande (CLI) de Systems Manager pour AMS Accelerate.	16 févr. 2023
Contenu mis à jour : ressources de gestion de l'intégration	Les modèles JSON compressés ont été mis à Le modèle pour créer des rôles AMS jour.	16 févr. 2023

Modification	Description	Date
Nouveau contenu : Conformité des configurations	Ajout d'un nouveau sujet :Constatations et réponses personnalisées.	16 févr. 2023
Nouveau : politiques AWS gérées.	Politique ajoutée :Rôle lié au service Amazon EventBridge Rule pour AMS Accelerate.	07 févr. 2023
Mise à jour : politiques AWS gérées.	Mise à jour `AWSManagedServices DeploymentToolkitPolicy` avec les nouvelles autorisations S3. Consultez Accélérez les mises à jour des rôles liés aux services.	30 janv. 2023
Nouvelle région opt-in : CPT.	AMS Accelerate est désormais disponible dans la région optionnelle du Cap (CPT). Pour vous inscrire, consultez la section Gestion Régions AWS.	12 janv. 2023
Mise à jour : Description du service.	Ajout de FSx services surveillés par des CloudWatch alarmes àService description (Description du service).	12 janv. 2023
Mise à jour : surveillance des métriques par défaut.	Ajout de 6 FSx alarmes àAlertes issues de la surveillance de base dans AMS.	12 janv. 2023
Mise à jour : modèles AMS.	Ajout de la fonction Personnaliser les notificat ions d'alarme Cloudwatch à. Motifs AMS	12 janv. 2023
Mise à jour : ressources de gestion de l'intégration.	Mise à jour du tableau des modèles, en ajoutant une ligne pour `ams-onboarding-ssm-execution-role` inLe modèle pour créer des rôles AMS.	12 janv. 2023
Mise à jour : Conformité de la configuration.	Informations supplémentaires pour demander des corrections personnalisées (dans la case Important) surConformité des configurations dans Accelerate.	12 janv. 2023

Modification	Description	Date
Mise à jour : Service-linked-role autorisations.	Autorisations anciennes ou dupliquées supprimées. Consultez Utilisation de rôles liés à un service pour AMS Accelerate.	15 déc. 2022
Mise à jour : gestion des correctifs, fenêtres de maintenance.	Ajout de conseils aux instructions de la console, étape 5, pour créer une fenêtre de maintenance. Consultez Création d'une fenêtre de maintenance depuis la console Systems Manager pour AMS Accelerate.	15 déc. 2022
Nouveau : section de gestion des correctifs.	Ajout d'une section pour les fenêtres de maintenance du Patch Tuesday. Consultez Créez une fenêtre de maintenance récurrente « Patch Tuesday » depuis la console AMS (recommandé).	15 déc. 2022
Mise à jour : AMS Resource Scheduler.	Le nom de la AWS CloudFormation pile a été mis à jour. Consultez Utilisation des ressources avec AMS Resource Scheduler.	15 déc. 2022
Mise à jour : Marquez vos ressources pour les sauvegarder.	Ajout de conseils pour l'utilisation d'AMS Resource Tagger. Consultez Étiquetez vos ressources pour appliquer les plans de sauvegarde AMS.	15 déc. 2022
Mis à jour : sélectionnez un plan de sauvegarde.	Indique quels plans offrent une sauvegarde continue. Consultez Sélectionnez un plan de sauvegarde AMS.	15 déc. 2022
Mise à jour : AMS Resource Scheduler.	Mise à jour de l'exemple de AWS CLI pour supprimer une période ou un calendrier. Consultez Utilisation des périodes et des plannings dans AWS Managed Services Resource Scheduler.	15 déc. 2022

Modification	Description	Date
Mise à jour : politiques AWS gérées.	A ajouté le`AWSManagedServices DeploymentToolkitPolicy` . Consultez AWS politiques gérées pour AMS Accelerate.	15 déc. 2022
Nouveau : Ajout d'une section décrivant le nouveau rôle lié au service AMS,. AWSServiceRoleForManagedServices_DetectiveControlsConfig	GovCloud Régions et autorisations ajoutées. Consultez Detective contrôle le rôle lié au service pour AMS Accelerate.	15 déc. 2022
Nouveau : AWS politique gérée	Ajout d'une section décrivant comment la politique AWS-managed, AWSManagedServices_AlarmManagerPermissionsBoundary, est utilisée dans la politique de rôle liée au service, AWSManagedServices_AlarmManager _ServiceRolePolicy, pour restreindre les autorisations des rôles IAM créés par le rôle lié au service. AWSServiceRoleForManagedServices_AlarmManager Consultez AWS politiques gérées pour AMS Accelerate.	15 déc. 2022
Mise à jour : Opérations à la demande.	Offres ajoutées : SQL Server on EC2 Operations et AMI Building and Vending. Consultez Opérations à la demande.	10 novembre 2022
Mise à jour : surveillance et gestion des événements.	Explication mise à jour des notifications de service et des rapports d'incidents. Consultez Fonctionnement de la surveillance.	10 novembre 2022
Mise à jour : régions de rôles liées à un service	GovCloud Régions et autorisations ajoutées. Consultez Utilisation de rôles liés à un service pour AMS Accelerate.	10 novembre 2022

Modification	Description	Date
Nouveau : rôle lié à un service.	Ajout d'un nouveau rôle :`AWSServiceRoleForAMSDetectiveControls` . Consultez Detective contrôle le rôle lié au service pour AMS Accelerate.	10 novembre 2022
Mise à jour : gestion des accès.	Sous-sections mises à jour avec des instructions améliorées. Consultez Gestion des accès dans AMS Accelerate.	10 novembre 2022
Mise à jour : description du service	Modèles AMS mis à jour dans la matrice RACI. Consultez Service description (Description du service).	10 novembre 2022
Mise à jour : modèles AMS.	Les clients sont responsables des déploiements de modèles. Consultez Motifs AMS.	10 novembre 2022
Mise à jour : Offboarding.	Ajout de détails sur ce qu'il advient de certaines ressources de sauvegarde et de surveillance lors du désenclavement. Consultez Déconnecter d'AMS Accelerate.	10 novembre 2022
Mise à jour : gestion des correctifs.	Directives actualisées et abrégées concernant les politiques IAM. Consultez Création d'un rôle IAM pour l'application de correctifs à la demande à AMS Accelerate.	10 novembre 2022
Nouveau : liens vers des schémas d'architecture.	Ajout de liens vers des diagrammes d'architecture de référence AMS vers divers sujets. Pour obtenir un exemple, consultez Surveillance et gestion des événements dans AMS Accelerate.	10 novembre 2022
Nouveau : offre d'opérations à la demande	Ajout de « Opérations de l'accélérateur de zone d'atterrissage ». Consultez Opérations à la demande.	13 octobre 2022

Modification	Description	Date
Mise à jour : gestion de la surveillance. Les alertes génèrent des rapports d'incidents, et non des demandes de service	Fonctionnement de la surveillance.	13 octobre 2022
Nouveau : Création d'une fenêtre de maintenance des correctifs avec un modèle CFN personnalisé pour Accelerate	AWS CloudFormation modèles de configura tion de fenêtre de correctifs. Consultez Création d'une fenêtre de maintenance des correctifs dans AMS.	15 septembre 2022
Mise à jour : Offboarding	A souligné que les plans de sauvegarde dans Accelerate ne fonctionnent plus après le déchargement. Consultez Déconnecter d'AMS Accelerate.	15 septembre 2022
Mise à jour : détails des modifications de CloudWatch configuration	Correction d'une erreur dans les exemples Windows et Linux. Consultez CloudWatch détails des modifications de configuration.	15 septembre 2022
Mise à jour : utilisation du planificateur de ressources AMS	Ajout de conseils sur les balises de répartition des coûts. Consultez Estimateur de coûts dans AMS Resource Scheduler.	15 septembre 2022
Mise à jour : bibliothèque de règles de configuration AMS	Ajout de deux règles de `ams-eks-` configura tion à la table des règles. Consultez Bibliothè que de règles de configuration AMS.	15 septembre 2022
Mise à jour : Backup Management	L'étiquette trompeuse PITR (point-in-time-recovery) a été supprimée des titres et des descriptions des plans de sauvegarde. Consultez Sélectionnez un plan de sauvegarde AMS.	15 septembre 2022

Modification	Description	Date
Mise à jour : description du service Accelerate	Descriptions mises à jour des règles de configuration et des canaris. Consultez Service description (Description du service).	15 septembre 2022
Mise à jour : description du service, configurations prises en charge	end-of-serviceDate de suppression pour Windows 2008 R2. Accelerate n'est pas compatible avec Windows 2008. Consultez Configurations prises en charge.	11 août 2022
Mise à jour : description du service, rôles et responsabilités	Mise à jour de la table RACI. Les journaux d'accès ELB ont été supprimés de la dernière ligne de la section Mise en réseau. Nous n'activons pas les journaux d'accès ELB pour les clients Accelerate. Consultez Rôles et responsabilités.	11 août 2022
Mise à jour : Conformité des configurations	Correction d'une faute de frappe dans la colonne Tableau des règles, cadres. Le NIST-CSF a été incorrectement répertorié comme NIST-CIS. Consultez Conformité des configurations dans Accelerate.	11 août 2022
Nouveau : Accélérez l'offboarding	Considérations et processus de désenclavement. Voir Offboarding AMS Accelerate.	11 août 2022
Mise à jour : liste des systèmes d'exploitation des agents SSM préinstallés	Ajout de « Ubuntu Linux 18.04 et 20.04 » à la liste. Consultez Intégrer des EC2 instances pour accélérer.	11 août 2022
Nouveau : planificateur de ressources	Utilisez le planificateur de ressources AMS pour optimiser les coûts en arrêtant et en démarrant les ressources uniquement lorsque cela est nécessaire. Consultez Optimisation des coûts avec AMS Resource Scheduler.	14 juillet 2022

Modification	Description	Date
Mise à jour : description du service pour le planificateur de ressources	Plusieurs sections de la description du service ont été mises à jour pour la nouvelle offre Resource Scheduler. Consultez Service description (Description du service).	14 juillet 2022
Nouveau : AMS Patterns	AMS propose des modèles de modèles, une solution généralisée qui répond à une famille de cas d'utilisation dans l'environnement géré AMS. Premier patron proposé :Motifs AMS.	14 juillet 2022
Nouveau : note sur l'optimis ation des coûts	Ajout d'une note expliquant comment les coûts peuvent augmenter avec l'utilisation des ressources. Consultez Inventaire des ressource s pour Accelerate.	14 juillet 2022
Mise à jour : règles de configuration AMS	Réorganisation des tables dans le. Bibliothè que de règles de configuration AMS Le tableau HTML comporte moins de colonnes, ce qui facilite sa lecture en un coup d'œil. La feuille de calcul téléchargeable comporte des colonnes supplémentaires pour permettre le tri et le filtrage.	14 juillet 2022
Mise à jour : gestion des accès	Le CloudFormation modèle d'exemple a été mis à jour dansAutorisations d'utilisation des fonctionnalités AMS. La `AMSAccele rateAdminAccess` politique inclut désormais les `IAMReadOnlyPolicy` politiques `AmsResourceSchedul erPassRolePolicy` et.	14 juillet 2022
Mise à jour : rapports en libre-service	Ajout d'instructions pour le chiffrement des AWS Glue métadonnées à l'aide de clés KMS. Voir la case intitulée Important surRapports en libre-service.	14 juillet 2022

Modification	Description	Date
Mise à jour : surveillance de base AMS	Alerte DeleteRecoveryPoint de sauvegarde ajoutée. Alertes issues de la surveillance de base dans AMS	14 juillet 2022
Mise à jour : Systèmes d'exploitation pris en charge	Date de fin de Support ajoutée pour Amazon Linux 2. Service description (Description du service)	14 juillet 2022
Mise à jour : AMS Reporting	Ajout d'une note concernant les régions optionnelles. Rapports et options	14 juillet 2022
Planificateur de ressources	Ajout d'informations sur l'intégration et l'utilisation d'AMS Resource Scheduler pour aider à optimiser les coûts en planifiant les heures d'arrêt et de début des ressources. J'ai également mis à jour la description du service Accelerate pour inclure la mention du planificateur de ressources. En outre, la date de fin du support pris en charge par Amazon Linux 2 a été mise à jour à 2024. Voir Optimisation des coûts avec AMS Resource Scheduler et Service description (Description du service)	30 juin 2022
Nouvelle alarme	Une AWS Backup alarme a été ajoutée. Alertes issues de la surveillance de base dans AMS	21 juin 2022
Nouveau contenu	Le contenu du rôle lié au service a été ajouté. Utilisation de rôles liés à un service pour AMS Accelerate	16 juin 2022
	AWS Network Firewall Operations a été ajoutée au catalogue d'offres Operations on Demand (OOD). Opérations à la demande	16 juin 2022

Modification	Description	Date
Contenu mis à jour	Ajout d'une description de la fonctionnalité de gestion des problèmes. Service description (Description du service)	16 juin 2022
	Ajout d'une note concernant l'ensemble de règles de configuration qui ne prend pas en charge certaines régions d'opt-in. Conformité des configurations dans Accelerate	16 juin 2022
	Conformité de la configuration. « Bibliothèque de règles de configuration AMS » -> « Table des règles », a été mise à jour et supprimée au format ZIP uniquement. Conformité des configurations dans Accelerate	16 juin 2022
	Suppression des e-mails d'escalade. Voie d'escalade	16 juin 2022
	La liste des sujets a été déplacée en dessous des paragraphes d'ouverture. Qu'est-ce qu'AMS Accelerate ?	16 juin 2022
	Le contenu de la réméditation automatique a été mis à jour. Correction automatique des alertes par AMS	16 juin 2022
Contenu mis à jour : Description du service	EKS a été ajouté à la liste des services surveillés par AMS Config Rules dansServices pris en charge. Description de surveillance mise à jour dans le tableau RACI dans. Rôles et responsabilités	12 mai 2022
Contenu mis à jour : Conformité des configurations	Ajout de règles de configuration liées à EKS. Consultez Conformité des configurations dans Accelerate.	12 mai 2022

Modification	Description	Date
Contenu mis à jour : Getting Started, Account Discovery	Ajout d'une version plus récente du AwsAccountDiscoveryCli script (dans le fichier zip Account Discovery Changelog) dans. Étape 1. Découverte de comptes dans Accelerate	12 mai 2022
Contenu mis à jour : surveillance, mesures par défaut	Conditions de déclenchement mises à jour pour les métriques liées à l'ALB. Consultez Alertes issues de la surveillance de base dans AMS.	12 mai 2022
Contenu mis à jour : intégration des correctifs	Ajout d'une condition préalable explicite à l'application des correctifs : vous devez vous inscrire à EBS. Consultez Intégration des correctifs dans Accelerate.	12 mai 2022
Contenu mis à jour : tableau d'inventaire des ressources accéléré	Modification des ams-detective-controls-config règles -rules-cdk, ajout de règles pour ams-detective-controls-recorder -cdk et -cdk. ams-detective-controls-infrastructure Consultez Inventaire des ressources pour Accelerate.	14 avril 2022
Contenu mis à jour : Conformité des configurations	Présentation des normes du secteur, des règles de configuration et des types de réponses. Souligne que les clients ne choisissent pas de règles de configuration ou de réponses individuelles. Conformité des configurations dans Accelerate.	14 avril 2022
Contenu mis à jour : Description du service	Déplacement de la section existante sur l'étendue des modifications sous Rôles et responsabilités. Consultez Rôles et responsabilités.	14 avril 2022

Modification	Description	Date
Contenu mis à jour : balisage et surveillance	Ajouté `AWS::Synthetics:Canary` aux listes des types de ressources autorisés pour le balisage et la surveillance. Consultez Profils de configuration de Resource Tagger dans AMS Accelerate et Accélérer le profil de configuration : substitution de pseudoparamètres.	14 avril 2022
Contenu mis à jour : Accelerate Preuisites	Les autorisations de bucket requises par le SMS ont été ajoutées à. Amazon EC2 Systems Manager dans Accelerate	14 avril 2022
Nouveau contenu : application de correctifs et surveillance	Ajout d'un exemple de code permettant d'utiliser Cloudformation pour déployer des configurations de balisage et de surveillance. Consultez Déploiement d'un profil de configuration avec AWS CloudFormation for Accelerate et Utilisation AWS CloudFormation pour déployer Accélérer les modifications de configuration.	10 mars 2022
Contenu mis à jour : console de maintenance des correctifs	Les étapes ont été réorganisées Création d'une fenêtre de maintenance depuis la console Systems Manager pour AMS Accelerate pour correspondre à l'interface de la console.	10 mars 2022
Contenu mis à jour : CLI de maintenance des correctifs	Paramètres de CLI mis à jour (calendrier, durée et limite) pour Créez une fenêtre de maintenance avec l'interface de ligne de commande (CLI) de Systems Manager pour AMS Accelerate	10 mars 2022
Nouveau contenu : Auto Instance Config	Ajout de la définition de « `AMSInstanceProfileBasePolicy` à » Informations relatives à la modification des autorisations IAM	10 mars 2022
Nouveau contenu : Onboarding	Ajout d'un exemple de commande Linux à Connectivité Internet sortante dans Accelerate	10 mars 2022

Modification	Description	Date
Nouveau contenu : Onboarding	Ajout d'une option de moindre privilège à. Le modèle pour créer des rôles AMS	10 mars 2022
Contenu mis à jour : instructions d'escalade accélérées	Ajout de conseils, de liens et de contacts par e-mail pour Voie d'escalade	10 mars 2022
Contenu mis à jour : configurations prises en charge	AMS prévoit de mettre fin au support de RHEL 6 CentOs le 14 mars 2023. Consultez Configurations prises en charge.	10 mars 2022
Contenu mis à jour : tableau des ressources	Ajout de rôles IAM d'accès AMS au tableau Inventaire des ressources pour Accelerate des ressources	10 mars 2022
Contenu mis à jour : Onboarding and Backup	Ajout d'instructions pour s'inscrire AWS Backup à et Intégration à AWS Backup Accelerate Gestion de la continuité dans AMS Accelerate	10 mars 2022
Contenu mis à jour : Gestion des accès	Les instructions spécifiques à Advanced ont été supprimées du guide Accelerate. Comment et quand utiliser le compte utilisateur root dans AMS	10 mars 2022
Contenu mis à jour : configurations prises en charge	AMS prend désormais en charge Oracle Linux 8.3 et Ubuntu 18.04 et 20.04. Consultez Configurations prises en charge.	28 février 2022
Contenu mis à jour : accord de niveau de service	Mise à jour du contrat de niveau de service téléchargeable dansServices pris en charge.	28 février 2022
Contenu mis à jour : Gestion des accès	Mise à jour Comment AMS accède à votre compte avec FAQs pour les rôles de console opérateur AMS et un avertissement de ne pas les modifier ou les supprimer.	28 février 2022

Modification	Description	Date
Contenu mis à jour : Alarm Manager	Mis à jour Accélérer le profil de configuration : surveillance. Alarm Manager n'est plus limité aux alarmes monométriques.	28 février 2022
Contenu mis à jour : Getting Started	Mis à jour Étape 2. Ressources de gestion de l'intégration dans Accelerate. Ajout d'un rôle IAM avec un accès minimal aux ressources d'intégration.	28 février 2022
Nouveau contenu : portée des modifications apportées à la description du service	Ajout d'une nouvelle section Étendue des modifications effectuées par AMS Accelerate qui met l'accent sur les limites et les actions qu'AMS Accelerate n'effectue pas.	10 février 2022
Contenu mis à jour : Getting Started	Le nouveau processus d'intégration commence par la configuration des fonctionnalités et des configurations par défaut avant la personnalisation. Les sous-sections contiennent des objectifs spécifiques aux fonctionnalités et des liens connexes. Consultez Commencer à utiliser AMS Accelerate.	10 février 2022
Contenu mis à jour : AMS Backup Management.	Le Gestion de la continuité dans AMS Accelerate chapitre a été raccourci et réorganisé pour plus de lisibilité.	10 février 2022
Contenu mis à jour : Balisage	Ajout d'une section Outils de balisage pour contenir des exemples de code CloudFormation et d'autres outils. Consultez Marquage dans AMS Accelerate.	10 février 2022
Contenu mis à jour : surveillance de base	L'amélioration des conditions de déclenchement de l'alarme RedShift du cluster réduit les fausses alarmes lors de la maintenance. Consultez Alertes issues de la surveillance de base dans AMS.	10 février 2022

Modification	Description	Date
Contenu mis à jour : application de correctifs	Exemple de commande CLI mis à jour pour enregistrer une fenêtre de maintenance. Consultez Créez une fenêtre de maintenance avec l'interface de ligne de commande (CLI) de Systems Manager pour AMS Accelerate.	10 février 2022
Contenu mis à jour : Inventaire des règles de AWS configuration.	La règle de configuration obsolète a été supprimée `ams-nist-cis-ec2-security-group-attached-to-eni` de la table d'inventaire des règles de AWS configuration. Consultez Tableau des règles.	27 janvier 2022
Nouveau contenu : création de fenêtres de maintenance des correctifs.	Ajout d'un lien vers le didacticiel SSM et des exemples de commandes pour créer des fenêtres de maintenance des correctifs à partir de la ligne de commande. Consultez Créez une fenêtre de maintenance avec l'interface de ligne de commande (CLI) de Systems Manager pour AMS Accelerate.	27 janvier 2022
Nouveau contenu : Resource Tagger reconnaît le nouveau type de ressource Auto Scaling Groups (ASG).	Ajout de groupes Auto Scaling aux types de ressources filtrables avec les profils de configuration Resource Tagger. Consultez Syntaxe et structure.	13 janvier 2022
Nouveau contenu : plans de sauvegarde et coffres-forts supplémentaires.	Ajout de nouveaux plans de sauvegarde et de nouveaux coffres-forts pour atténuer les scénarios à haut risque, notamment les attaques par ransomware. Consultez Afficher les sauvegardes dans les coffres-forts AMS et Afficher les sauvegardes dans les coffres-forts AMS.	13 janvier 2022

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.